SSL VPN 用户手册

天融信

TOPSEC®

北京市海淀区上地东路 1 号华控大厦 100085

电话：+8610-82776666

传真：+8610-82776677

服务热线：+8610-800 810 5119

http://www.topsec.com.cn

版权声明

本手册中的所有内容及格式的版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有　不得翻印©　2009 天融信®

商标声明

本安装手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC®　天融信®

信息反馈

http://www.topsec.com.cn

目　录

1 前言 1

1.1 文档目的 1
1.2 读者对象 1
1.3 文档基本内容 1
1.4 约定 2
1.5 相关文档 2
1.6 技术服务体系 2

2 SSL VPN客户端概述 4

3 使用网页浏览器 6

3.1 登录/退出网关 6
3.1.1 登录网关 6
3.1.2 退出网关 30
3.2 介绍用户主界面 32
3.3 设置页面风格 33
3.4 修改用户密码 35
3.5 访问内网资源 37
3.5.1 Web转发 37
3.5.2 端口转发 38
3.5.3 全网接入 41
3.5.4 应用WEB化 43
3.6 配置WEB SSO和日志级别 49
3.7 查看和配置客户端状态 51

4 使用独立客户端 53

5 使用PDA 64

1前言

安装天融信 SSL VPN 引擎的网络卫士防火墙，具备一切 SSL VPN 网关的功能，可作为一台标准的 SSL VPN 网关使用。SSL VPN 网关的普通用户可以在授权范围内进行资源访问。被授权的普通用户可以通过网页浏览器、SSL VPN 独立客户端或者 PDA（Personal Digital Assistant，个人数码助理，一般指掌上电脑）直接与网关建立连接，从而实现对内部被授权资源的访问。

本手册主要介绍天融信 SSL VPN 网关的普通用户操作部分说明。主要内容包括：用户登录和内网资源的使用。通过阅读本文档，用户可以根据访问权限在远程使用系统设置的各种资源。

1.1文档目的

本文档主要介绍普通用户如何使用 SSL VPN 网关，普通用户可以在本文档的指导下远程登录网关，然后使用授权资源。

1.2读者对象

本文档适用普通的具有基本网络知识的用户阅读，通过阅读本文档，可以独自完成以下应用操作：

- 登录 SSL VPN 网关
- 访问 Web 转发资源
- 访问端口转发资源
- 访问全网接入资源
- 访问应用 Web 化资源

1.3文档基本内容

本用户手册包含以下章节及附录：

- 第一章“前言”：主要介绍文档目的、读者对象、文档基本内容、文档中的文字及图片的约定、相关文档，以及如何获取技术支持的信息。
- 第二章“SSL VPN 客户端概述”：简单介绍 SSL VPN 客户端。
- 第三章“使用网页浏览器”：主要介绍如何使用网页浏览器登录网关的用户界面，如何安装客户端控件，如何访问内网资源，如何配置单点登录，以及如何查看 SSL VPN 客户端状态和登录信息。
- 第四章“使用独立客户端”：主要介绍如何在用户主机中安装 SSL VPN 独立客户端，如何使用独立客户端登录网关，如何访问内网资源。
- 第五章“使用 PDA”：主要介绍如何在 PDA 中安装 SSL VPN 独立客户端，如何使用独立客户端登录网关，如何访问内网的全网接入资源。

1.4约定

图形界面操作的描述采用以下约定：

按钮用“”表示，菜单项用宋体加粗字体表示。

点击（选择）一个菜单项采用如下约定：

点击（选择） **高级管理 > 特殊对象 > 用户**。

文档中出现的提示、警告、说明、示例等，是关于用户在安装和配置过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。

1.5相关文档

《NGFW 管理手册——基础配置》

《NGFW 管理手册——SSL VPN 配置》

《NGFW 命令行手册——SSL VPN 配置》

1.6技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

http://www.topsec.com.cn/

在线技术资料

http://www.topsec.com.cn/support/down.asp

安全解决方案

http://www.topsec.com.cn/solutions/qw.asp

技术支持中心

http://www.topsec.com.cn/support/support.asp

天融信全国安全服务热线

800-810-5119

2SSL VPN 客户端概述

用户登录 SSL VPN 网关后，可以通过不同的方式访问后台的授权资源，主要包括：WEB 转发方式，端口转发方式，全网接入方式和应用 WEB 化方式。“WEB 转发”和“应用 WEB 化”方式无需任何控件和组件的支持，“端口转发”和“全网接入”方式则需要下载并安装天融信下载管理控件和端口转发或全网接入组件，否则用户既使登录成功，也无法访问相应的授权资源。需要注意的是：（1）用户访问授权资源的方式由网关管理员的配置所决定；（2）目前，天融信 SSL VPN 网关不支持网关管理员为用户同时开启端口转发方式和全网接入方式。

目前，SSL VPN 网关允许用户主机使用 Windows 操作系统和非 Windows 操作系统登录然后访问授权资源。Windows 操作系统包括 Windows2000、WindowsXP、Windows2003、vista 和 Windows2008，并且可以支持控件模块（即“端口转发”模块和“全网接入”模块）；非 Windows 操作系统，如苹果系统，Linux 系统等，不支持控件模块。本文档主要以 Windows 操作系统为例，介绍用户操作，所以，如无特殊说明，下述所有描述和操作均基于 Windows 操作系统平台。

使用 Windows 操作系统的用户可以通过以下三种方式登录 SSL VPN 网关：

- 网页浏览器（安装在客户端主机中）

  网页浏览器包括IE浏览器（6.0 以上版本）和非IE浏览器，IE浏览器支持SSL VPN 网关所有的功能模块；非IE浏览器仅支持非控件模块。用户使用网页浏览器的具体操作请参见 3使用网页浏览器 的详细描述。

- 独立客户端（安装在客户端主机中）

  独立客户端支持所有功能模块。用户使用独立客户端的具体操作请参见 4使用独立客户端 的详细描述。

- PDA

  PDA（Personal Digital Assistant，个人数码助理，一般指掌上电脑）必须基于 Windows Mobile 6.0 以上版本的操作系统，并且仅支持“全网接入”模块。用户使用PDA登录网关的具体操作请参见 5使用PDA 的详细描述。

说明

✧ 用户不能同时运行“独立客户端”和“网页浏览器”登录 SSL VPN 网关。

3使用网页浏览器

由于非 IE 浏览器不支持控件模块，只能访问授权的“WEB 转发”资源和“应用 WEB 化”资源，所以本章以 6.0 版本的 IE 浏览器为例，介绍用户如何使用网页浏览器登录网关，然后访问授权资源，主要内容包括：

- 登录/退出网关
- 介绍用户主界面
- 设置页面风格
- 修改用户密码
- 访问内网资源
- 配置 WEB SSO 和日志级别
- 查看和配置客户端状态

3.1登录/退出网关

3.1.1登录网关

普通用户在进行登录前，建议提前进行以下操作：

1）确认用户主机中 IE 浏览器的版本：IE6.0 及其以上版本。

2）用户浏览器必须支持 SSL VPN 网关使用的 SSL 协议（SSLv3.0 或 TLSv1.0），请向管理员咨询待接入网关支持哪种 SSL VPN 协议类型。在用户浏览器中选择 SSL 协议的操作如下所示：

在 IE 浏览器中，点击 **工具 > Internet 选项**，然后选择“高级”页签，在“安全”项中勾选“使用 SSLv3.0”或“使用 TLSv1.0”，建议两种都选择。

3）导入证书信任链。

用户在登录SSL VPN网关之前，SSL VPN网关使用网关证书向用户浏览器进行认证，用户浏览器可以通过证书信任链来验证该网关证书的合法性。下载证书信任链的操作请参见 下载证书链 的相关描述，下面主要介绍如何导入证书信任链：

在 IE 浏览器中，点击 **工具 > Internet 选项**，然后激活“内容”页签，点击“证书”按钮，然后再激活“受信任的根证书颁发机构”页签，点击“导入”按钮，最后根据提示将“.P7B”格式的证书信任链导入到用户浏览器中。

说明

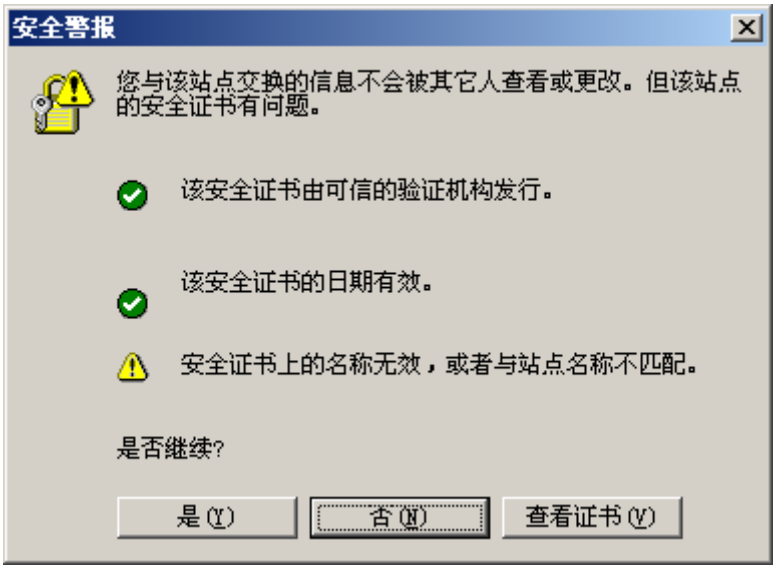
- ✧ 将网关的 CA 证书导入到 web 浏览器的“受信任的根证书颁发机构”中后，也可以对网关证书进行验证，但是必须保证网关 CA 证书的合法性，否则，使用不合法的网关 CA 证书来验证网关证书是没有意义的。
- ✧ 在 SSL VPN 网关中，证书信任链的下发功能极大地方便了用户操作，用户无需向网关管理员索要证书信任链。
- ✧ 如果网关证书是用户浏览器所信任的颁发机构签发的，无需导入证书信任链或者合法的网关 CA 证书。
- ✧ 网关证书的名称必须与站点名称相一致（例如，用户连接网关时输入的 URL 为“https://192.168.83.236”，那么该网关证书的名称必须为“192.168.83.236”），否则，即使导入了证书信任链或者网关的 CA 证书，用户浏览器仍然会弹出“安全警告”窗口，提示用户该网关的安全证书有问题。

普通用户通过 IE 浏览器初次登录网关的具体操作步骤如下所示（以 IE6.0 浏览器为例）：

1．进入用户登录页面。

打开 IE 浏览器，然后在地址输入框中输入形如 https://xxx. xxx. xxx. xxx 的网关连接地址（该地址由管理员提供给用户）。

如果浏览器中未正确导入合法的证书信任链或网关的 CA 证书，将弹出“安全警报”对话框，形如下图所示。



SSL 客户端确认 SSL VPN 网关身份时，主要根据以下标准来判断网关证书是否有效：

a）网关证书的根 CA 必须是用户浏览器所信任的。

b）当前的日期和时间必须在网关证书的有效期内，而且也必须在证书信任链中所有 CA 证书的有效期内。

c）网关证书的名称必须与站点名称一致。例如，用户连接网关时输入的 URL 为“https://192.168.83.236”，那么该网关证书的名称必须为“192.168.83.236”。

如果网关证书完全符合以上三点，用户浏览器认为该网关是可以信任的，于是直接进入用户登录界面；否则弹出上图的“安全警告”窗口，此时，用户只有点击“是”按钮，忽略警告，才能进入站点。

说明

- ✧ 由于管理员在 SSL VPN 网关上可以设置的不同的页面风格，因此不同的用户可能将看到不同的登录界面和使用界面。

2．选择中英文用户界面。

进入站点后，通过点击界面右上方的“English”或“中文”链接，可以在中、英文用户界面之间进行切换。

3．智能选路。

1）自动选路模式下，用户在网页浏览器中输入“https://链路地址”后，将自动弹出测速对话框，对话框中显示了多条线路的访问连接及其链路延时，如下图所示。

如果实际链路已经添加到链路表中，则五秒钟后将自动关闭该测速对话框，同时连接到最优线路进行访问。否则，管理员配置的各个链路将都不可达而导致选路超时，用户需要手动关闭测速对话框，然后自动连接到默认链路（即地址输入框中输入的链路）。

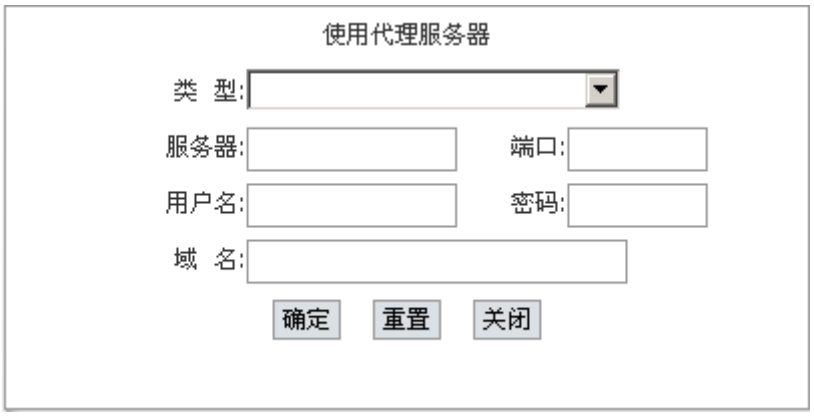
2）手动选路模式下，用户在网页浏览器中输入“https://链路地址”后，进入默认链路（即地址输入框中输入的链路）的用户登录界面。点击登录页面中的“手动测速”链接，进入手动选路界面中，该界面中显示了多条线路的访问连接及其链路延时。如下图所示。

测速完毕后，如果实际链路已经添加到链路表中，则用户可以手动选中某条链路名称，从而跳转到该线路进行访问；否则，用户需要手动关闭选路对话框，将自动连接到默认链路（即地址输入框中输入的链路）。

4．配置代理服务器。

对于天融信 SSL VPN 网关提供的端口转发或全网接入服务，用户可以通过代理服务器去连接网关，并通过代理服务器与 SSL VPN 网关建立 TCP/SSL 连接，然后访问相应授权资源。天融信 SSL VPN 网关允许用户使用的代理服务器的代理协议类型主要包括 HTTP、HTTPS 和 SOCKS，并且支持用户在客户端手动配置代理服务器，具体操作步骤如下所示：

1）用户打开登录页面后，选中“使用代理服务器”左侧的复选框，弹出“使用代理服务器”窗口，如下图所示。



界面参数说明如下表所示。

参数	说明
类型	选择用户所使用的代理服务器的代理协议类型。 可选值：与 IE 浏览器一致，Https 代理服务器，Socks 代理服务器。 说明： 1）“与 IE 浏览器一致”是指用户使用 IE 浏览器中配置的代理服务器去连接 SSL VPN 网关，此时，不能再设置该界面中其他参数，直接点击“确定”按钮使配置生效即可。 2）在 IE 浏览器中设置代理服务器的 IP 和端口号：在 IE 浏览器窗口中选择菜单项 **工具 > Internet 选项**，然后激活“连接”页签，点击“局域网设置”按钮进行配置。
服务器/端口	配置代理服务器的 IP 地址和端口号。 说明： 只有“类型”为“Https 代理服务器”或“Socks 代理服务器”时，才能够配置该参数。
用户名/密码	设置代理服务器授权的用户名和用户密码。 说明： 1）只有“类型”为“Https 代理服务器”或“Socks 代理服务器”时，才能够配置该参数。 2）有些代理服务器无需配置该参数。
域名	输入代理服务器所在的域。 说明： 1）只有“类型”为“Https 代理服务器”或“Socks 代理服务器”时，才能够配置该参数。 2）有些代理服务器无需配置该参数。

2）点击“重置”按钮，清空“使用代理服务器”页面中的所有配置，用户可以重新输入。

3）参数配置完成后，点击“确定”按钮使配置生效。

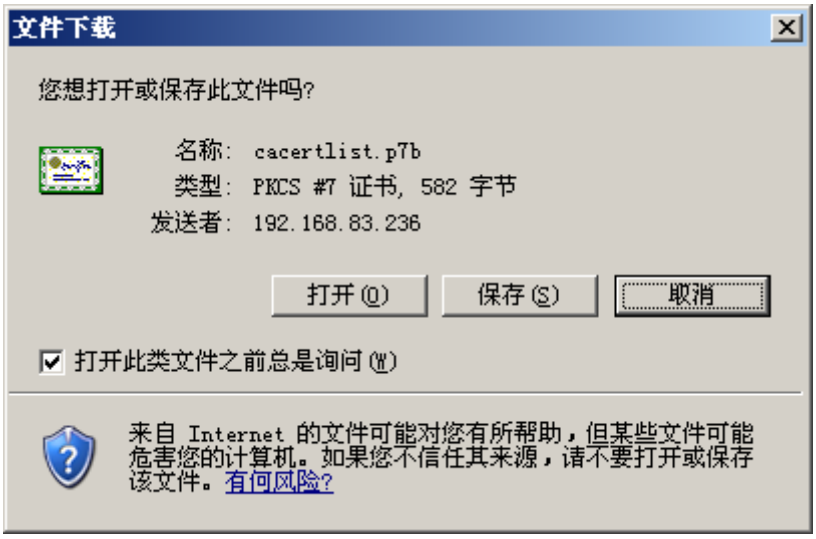
4）点击“关闭”按钮，关闭“使用代理服务器”页面。

5．下载证书链。

天融信 SSL VPN 网关的证书信任链主要是由一系列的 CA 证书组成的，其中包含了网关的 CA 证书，并最终以可信根 CA 证书结束。一般情况下，Web 浏览器已预先配置了一组浏览器自动信任的根 CA 证书，对于来自其他证书授权机构的网关证书，只有导入了该网关的证书信任链，用户浏览器才能检验该证书的有效性。因此，用户登录网关前，需要在用户浏览器中导入 SSL VPN 网关的证书信任链，并且网关中网关证书的名称必须与用户访问的站点名称一致，否则，浏览器将弹出“安全警告”窗口，提示用户该站点的安全证书有问题。

管理员事先已经将 SSL VPN 网关的证书信任链上传到网关中，用户只需下载并导入该证书信任链即可，具体操作如下所示：

1）用户打开登录页面后，点击“证书链下载”链接，弹出“文件下载”窗口，如下图所示。



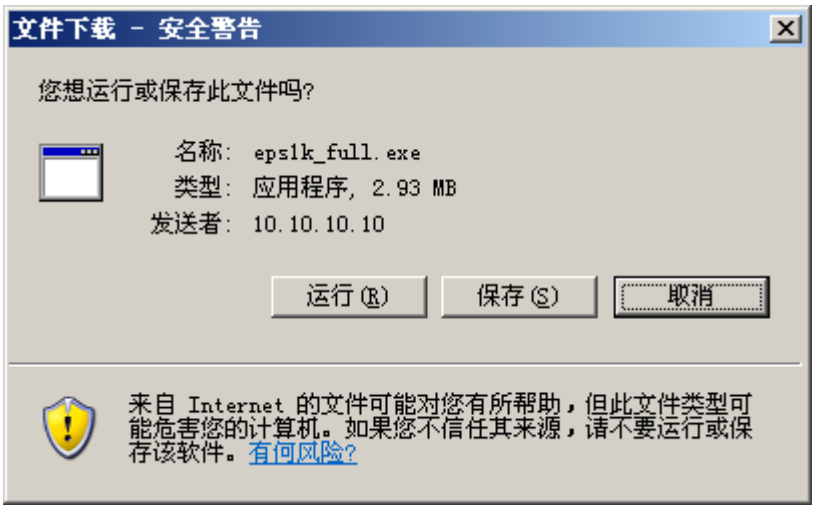
2）点击“保存”按钮，下载该证书链。

3）用户成功下载证书链后，将其安装在用户浏览器中即可，具体操作请参见 导入证书信任链。

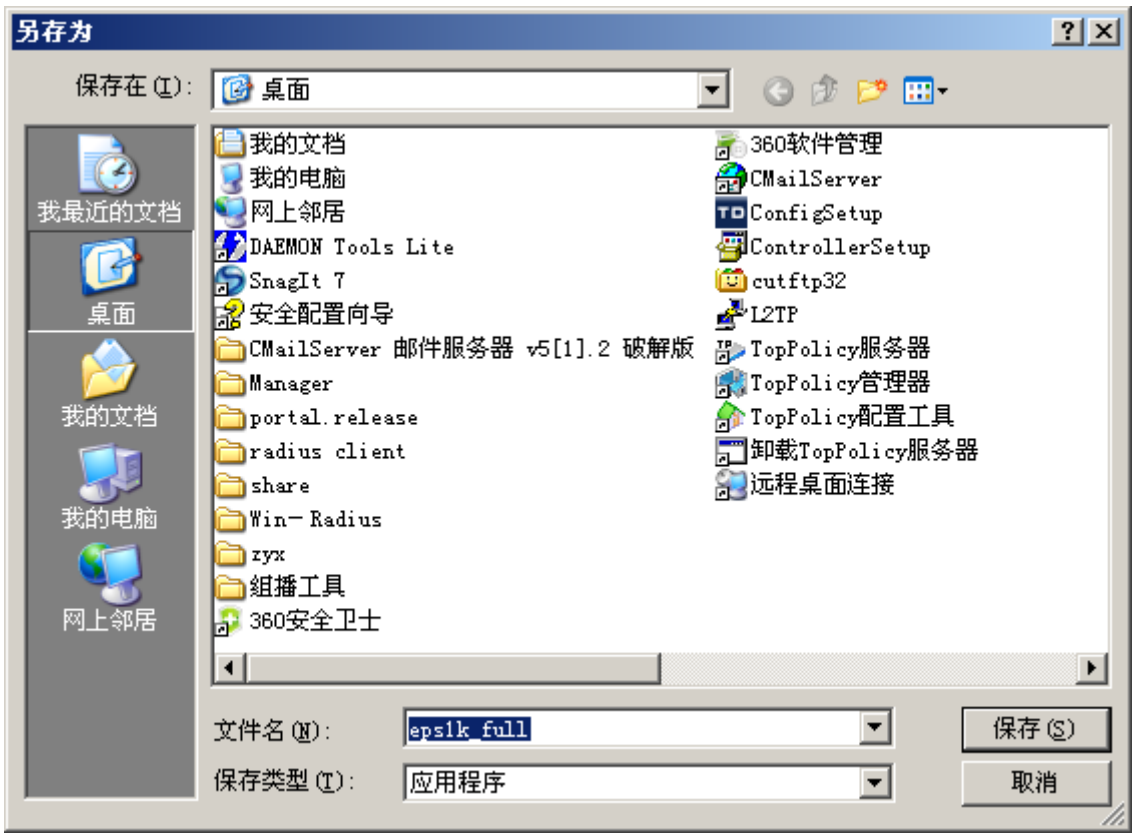
6．下载 USB 驱动。

SSL VPN 网关的用户界面中提供了 USB 驱动的下载功能，方便用户下载、安装。管理员事先已经将某个 USB 驱动上传到后台的 web 服务器中，下载该 USB 驱动的具体操作如下所示：

1）用户打开登录页面后，点击“USB 驱动下载”链接，弹出“文件下载”窗口，如下图所示。



2）点击“保存”按钮，弹出文件保存窗口，如下图所示。



3）选择保存路径后，点击“保存”按钮即可将该 USB 驱动下载到本地，等待后续安装。

7．找回密码。

SSL VPN 网关为本地认证用户提供了密码找回功能，如果管理员添加本地用户时配置了该用户的邮箱地址或手机号码，则用户执行密码找回操作后，网关将密码发送到用户邮箱或手机中，便于用户能够及时找到密码。找回密码的具体操作如下所示：

1）在用户登录页面中，点击“密码”文本框右侧的“忘记密码”链接，弹出窗口如下图所示。

为了防止重放攻击，网关需要用户执行密码找回操作时输入简单的验证码。

2）输入用户名和验证码后，点击“确定”按钮，网关即可将用户密码发送到用户邮箱或者手机中。

网关对用户的密码找回操作进行累计，允许用户连续查询 10 次，超过该次数后，网关将拒绝执行该操作。只有在用户登录成功之后，网关才会清除密码找回计数累计。

3）点击“关闭”按钮，关闭该窗口。

8．图形认证码。

为了预防口令的暴力破解攻击，SSL VPN 网关支持用户界面的图形认证码识别功能。如果管理员配置了“不显示”图形认证码，则用户界面永远不会显示验证码信息；如果管理员配置了“总显示”图形认证码，则用户需要在登录界面中输入验证码信息；如果管理员配置了“登录失败三次后显示”图形认证码，则用户输错三次登录信息后，网关自动生

成认证码，当用户再次登录时必须提供认证码信息。需要用户提供图形认证码的登录界面形如下图所示。

说明

- ✧ 根据管理员对图形认证码显示方式的设置，登录界面中将总显示、不显示或登录失败三次后显示图形认证码的输入框。

9．用户身份认证。

普通用户登录 SSL VPN 网关时，可以通过口令、证书、双因子（即：口令+证书）的方式进行身份认证。但是，当管理员在 SSL VPN 网关上启用了“强制双因子认证”功能后，用户必须使用双因子认证方式，并且本地数据库中必须有一个采用“口令+证书”进行认证的同名用户，否则用户无法通过 SSL VPN 网关访问可用资源。

根据管理员在 SSL VPN 网关上设置的“登录设置”的不同，普通用户可以有三种不同方式的登录操作。

1）口令认证。

对于口令认证用户，需要在“口令认证”页签中输入登录信息，如下图所示。

a）在该登录界面中，输入管理员设置的用户名和密码。

SSL VPN 网关用户界面中提供了使用软键盘输入密码的功能，用于防止木马盗取密码，极大地提高了用户密码的安全性。使用软件盘输入密码的方法如下所示：

① 点击图标“ ”，打开软件盘，如下图所示。

② 通过软键盘输入密码后，点击“确定”按钮即可完成。

点击“切换大/小写”按钮，可以转换软键盘上字符的大小写；点击“退格”按钮，可以删除软键盘输入的字符；点击“禁用键盘输入”按钮，可以退出软键盘输入方式。

b）登录信息设置完成后，点击“确定”按钮进入用户界面。

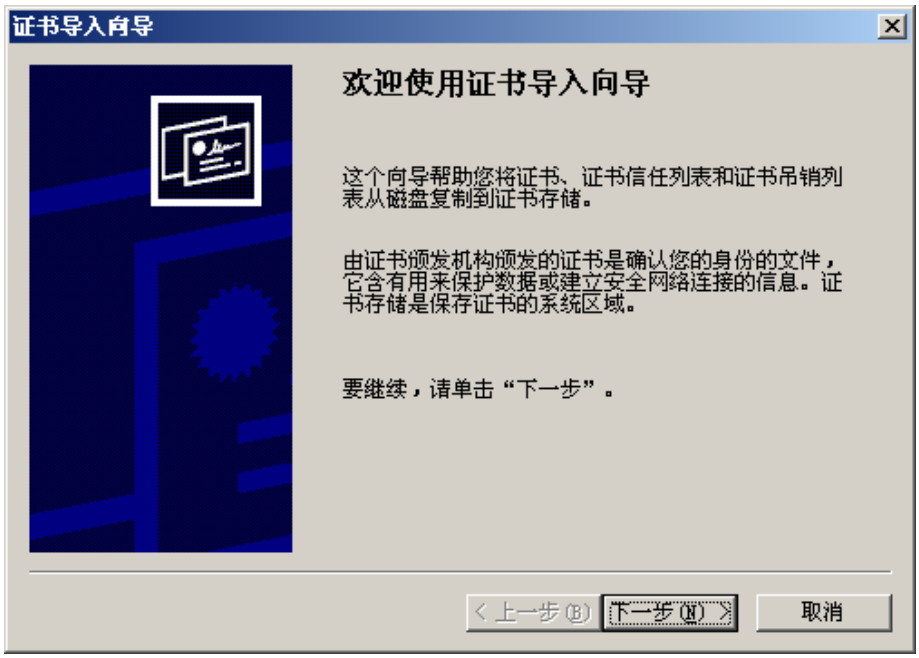
2）证书认证。

对于证书认证用户，需要在“证书认证”页签中输入登录信息，如下图所示。

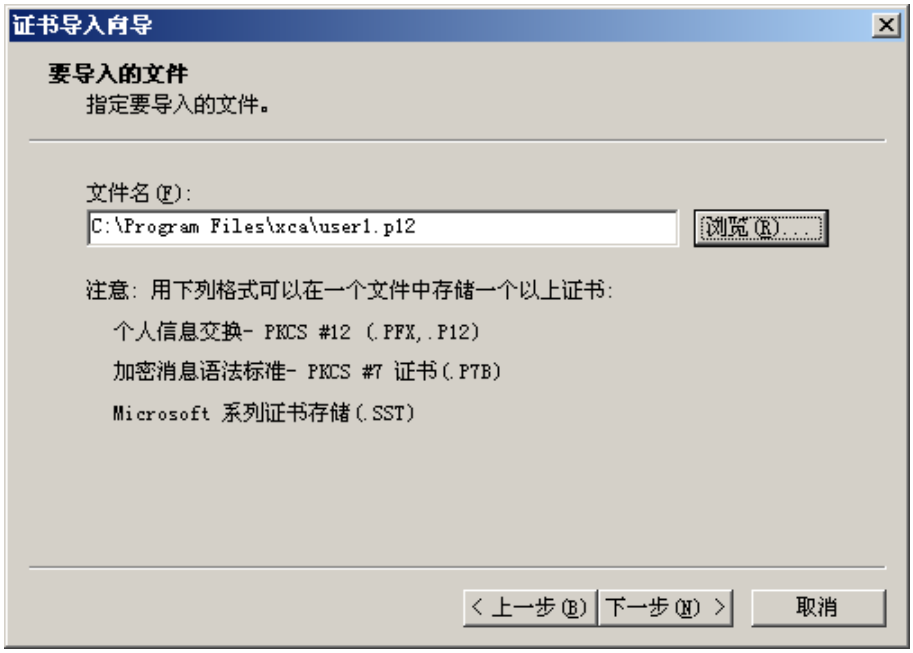
在该登录界面中，点击“证书认证”按钮，选择正确的用户证书进入用户界面（既可以使用浏览器中安装的用户证书，也可以使用 USBKey 中保存的用户证书）。

a）当使用浏览器中安装的证书文件进行登录时，用户需要由管理员处获得证书文件，并把证书安装到浏览器中，证书安装及认证过程如下（以 IE 浏览器为例）：

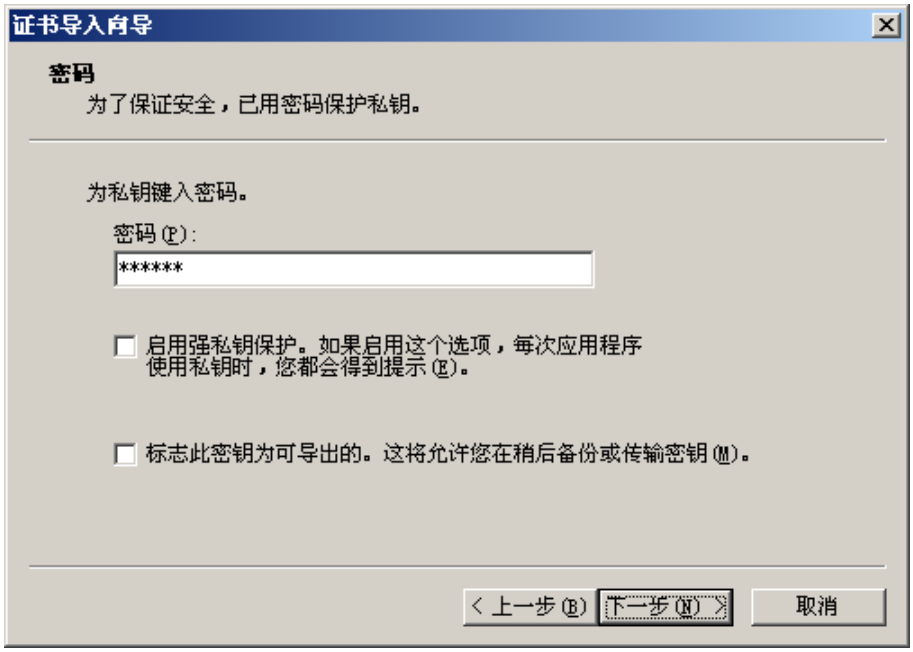
① 用户获得证书后，双击证书文件或选中证书文件，单击鼠标右键，选择“PFX 安装”，用户可以按照提示安装证书。如下图所示。



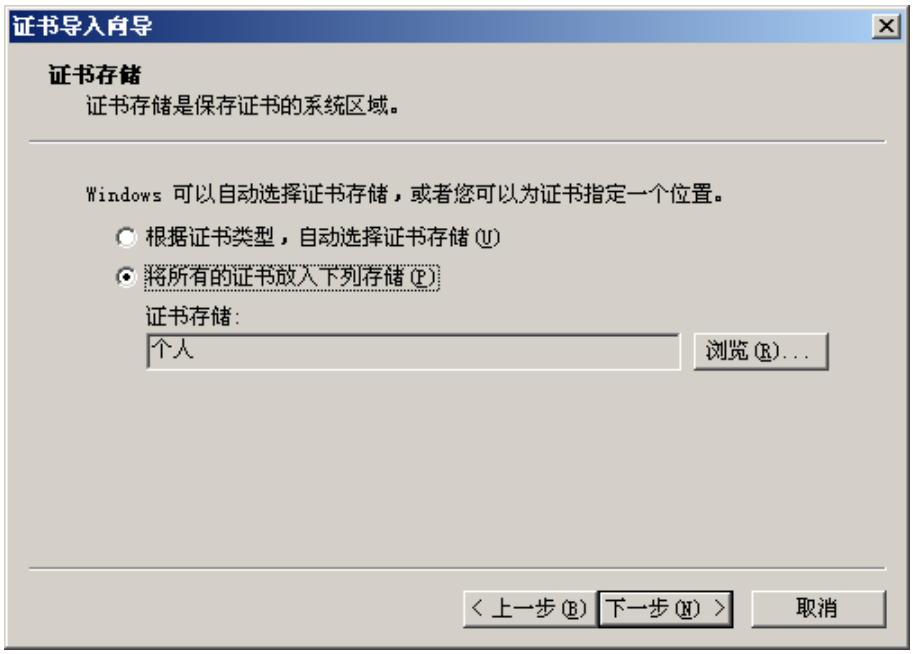
② 点击“下一步”按钮，在下图所示对话框中填写证书存放路径，或点击“浏览…”进行查找。



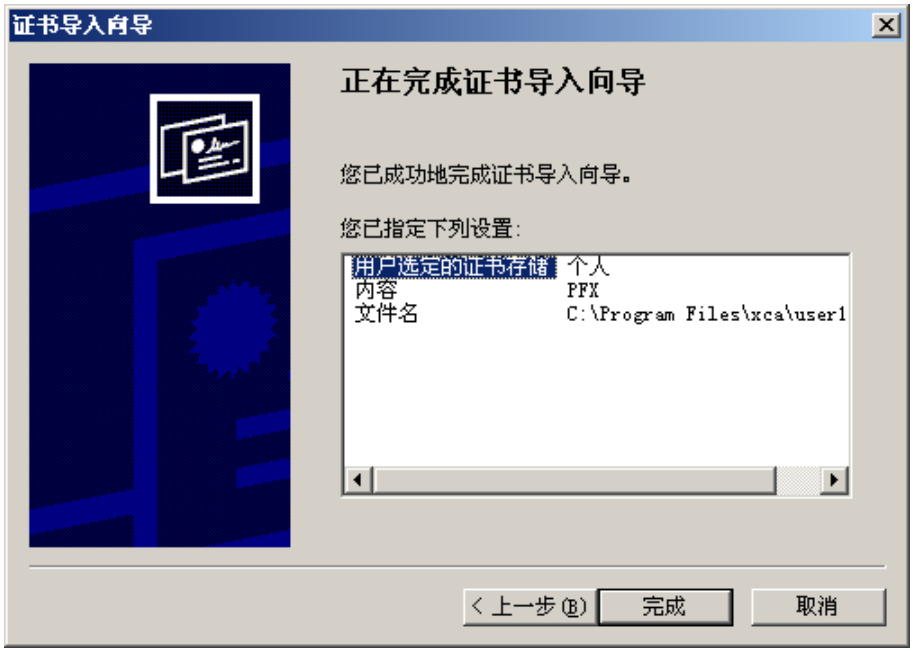
③ 点击“下一步”按钮，在下图对话框中输入证书导出时设置的保护密码。如果管理员在导出证书时设置了密码则此处必须输入该密码。没有获得证书导出密码的用户可向管理员索取。



④ 点击“下一步”按钮，在下图所示对话框中选择存储区域。

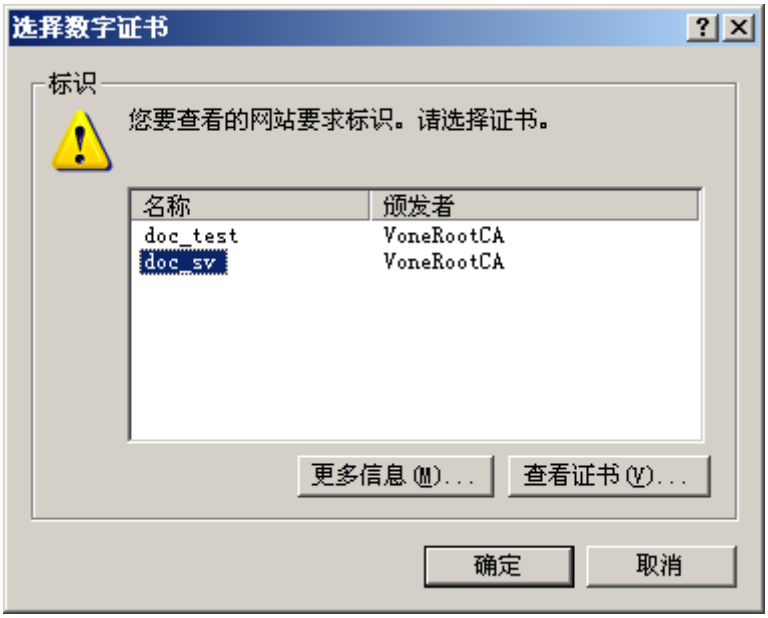


⑤ 点击“下一步”按钮，完成用户证书的导入，如下图所示。



⑥ 点击“完成”按钮，弹出证书导入成功的提示框，如下图所示。

⑦ 在用户登录页面中，点击“证书认证”按钮后，弹出“选择数字证书”对话框，如下图所示。



⑧ 选中用户证书，然后点击“确定”按钮，即可成功登录用户界面。

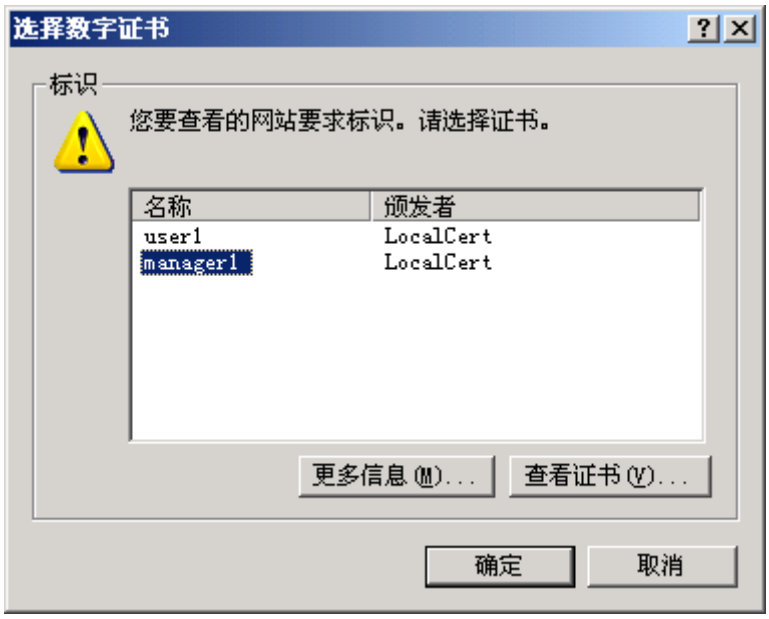
b）当使用 USBKEY 保存的用户证书进行登录时，用户需要由管理员处获得保存证书的 USBKey（目前仅支持 epass1000）及相应的驱动程序。如果用户使用天融信公司的 TOPKEY 产品，则可以从网关的随机光盘上找到相应的驱动程序；用户也可以在用户界面中下载 SSL VPN 网关中保存的 USB 驱动程序，该 USB 驱动事先由管理员上传到网关中。

使用 USBKEY 保存的用户证书进行登录的具体操作过程如下所示：

① 安装 epass1000 的驱动程序。

② 将装有证书的 epass1000 插入主机的 USB 接口。

③ 在用户登录页面中，点击“证书认证”按钮后，弹出选择证书界面，如下图所示。



④ 选择用户证书后，点击“确定”按钮，弹出验证用户 PIN 码的对话框，如下图所示。

⑤ 输入用户 PIN 后（PIN 码可由管理员处获得），点击“登录”按钮即可成功登录到用户界面中。

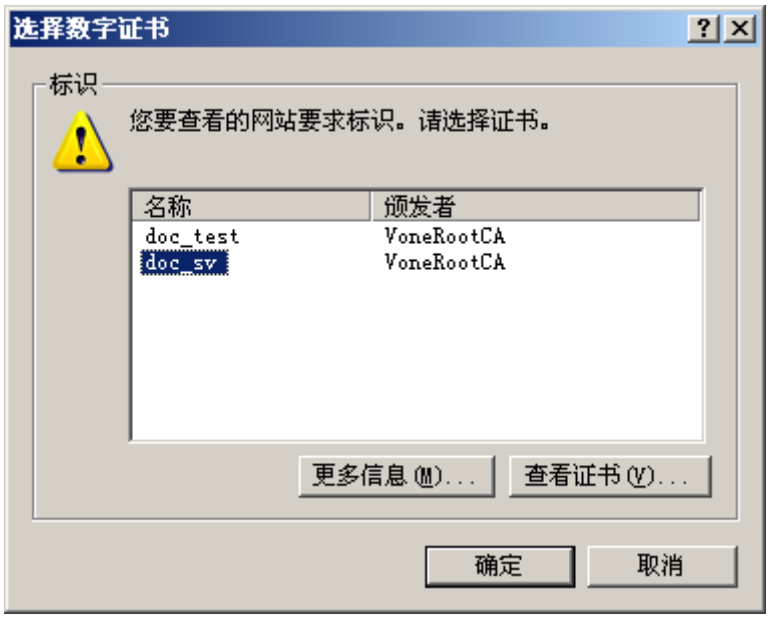
3）双因子认证。

对于双因子认证用户，需要在“双因子认证”页签中输入登录信息，具体认证步骤如下所示：

a）将用户证书导入到用户浏览器中，具体介绍请参见 证书认证 的相关介绍，此处不再赘述。

b）激活“双因子认证”页签，输入用户名和密码信息，如下图所示。

c）点击“登录”按钮，弹出“选择数字证书”窗口，要求用户选择用户证书，如下图所示。



d）在“选择数字证书”窗口中选中用户证书，然后点击“确定”按钮。

e）在“双因子认证”页签中，点击“登录”按钮即可成功登录用户使用界面。

说明

- ✧ 如果管理员启用了加密卡功能，并且加载了加密卡，则用户登录前必须插入支持相应硬件算法的 USBKEY，否则 SSL VPN 客户端和 SSL VPN 网关之间无法加密通信数据，导致用户无法登录网关。

10．短信认证。

如果网关管理员开启了“强制短信认证”，用户身份合法性认证通过后，网关会发送一条包含随机序列码的短信到该用户手机，同时要求用户进行短信认证。

在弹出的对话框中输入手机短信中正确的序列码，短信认证通过后，远程用户才能成功登录 SSL VPN 网关用户界面。

11．安装控件和组件。

用户初次登录网关，并进入用户使用界面后，网关首先会提示用户安装天融信下载管理控件，只有正确安装了天融信下载管理控件后，网关才能继续提示用户下载并安装客户端组件，包括天融信端点安全组件，天融信全网接入组件和天融信端口转发组件。

说明

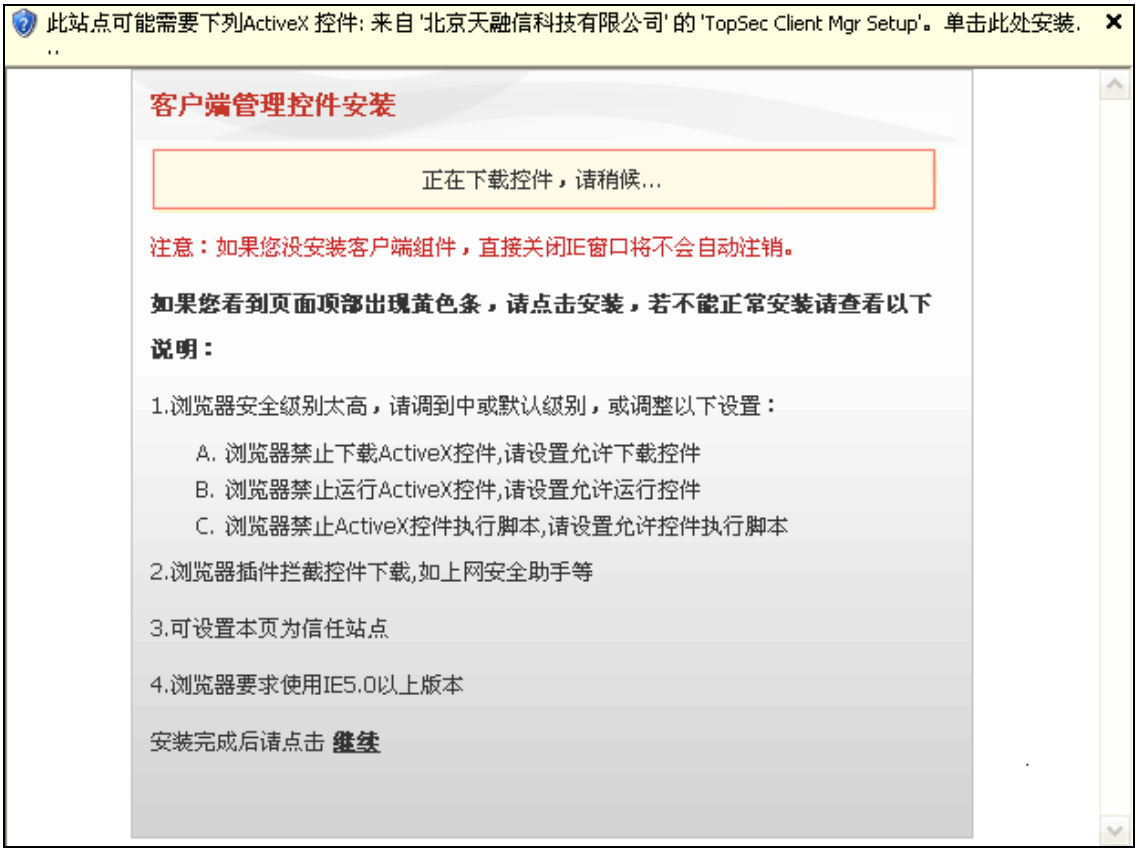
- ✧ 如果管理员不允许用户安装控件，则用户不能安装“天融信下载管理控件”和任何客户端组件，登录成功后直接进入用户使用界面，既不能访问端口转发资源和全网接入资源，也不能使用端点安全功能（即：访问结束后，无法消除客户端浏览器的历史纪录等）。
- ✧ 如果管理员允许用户安装控件，并且为该用户开启了端口转发模块和全网接入模块，则用户初次成功登录网关后，必须按照提示信息安装天融信下载管理控件、端点安全组件、端口转发客户端组件、全网接入客户端组件，然后才能访问授权资源。
- ✧ 如果管理员允许用户安装控件，但是并没有为该用户开启端口转发模块（或全网接入模块），则用户初次成功登录网关后，可以按照提示信息安装天融信下载管理控件、端点安全组件，但是不能安装端口转发客户端组件（或全网接入客户端组件），继而不能访问授权的端口转发资源（或全网接入资源）。

天融信下载管理控件和 SSL VPN 客户端组件的安装步骤如下所示：

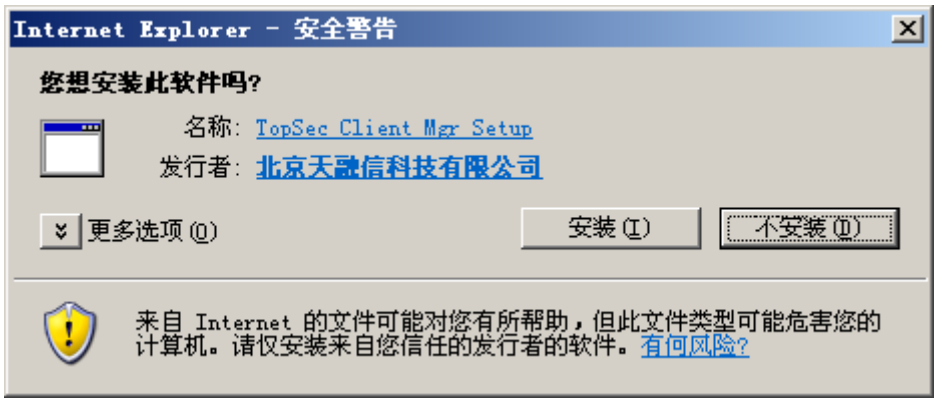
1）网关提示用户安装天融信下载管理控件：此步骤分为自动安装和手动安装进行介绍。

a）自动安装。

如果管理员配置的控件安装方式为“自动安装”，则用户成功登录网关后，网关将弹出如下界面，提示用户安装“天融信下载管理控件”。



点击页面顶部出现的黄条，然后选择右键菜单项“安装 ActiveX 控件”，弹出安全警告窗口，如下图所示。



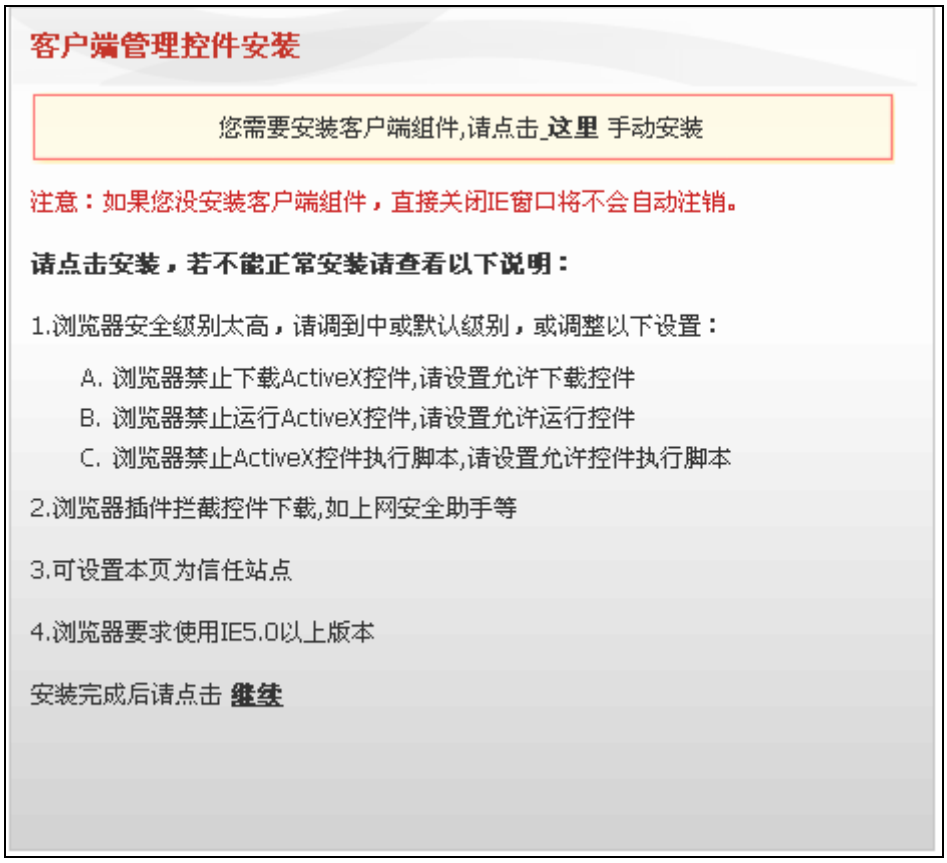
点击“安装”按钮，开始安装“天融信下载管理控件”，进入步骤 2）。

说明

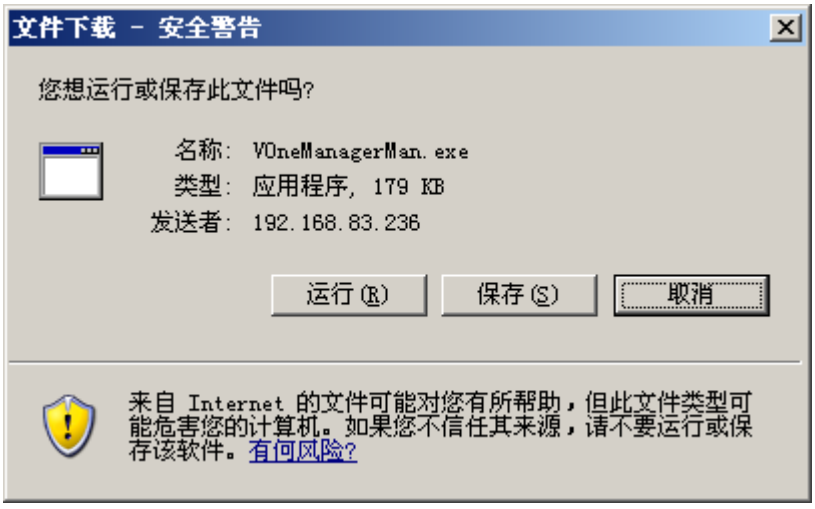
- 自动安装方式下，根据用户浏览器中安全级别设置的不同，可能不会出现黄条进行提示，而是在用户登录后网关自动开始安装“天融信下载管理控件”，即直接进入步骤 2）。

b）手动安装。

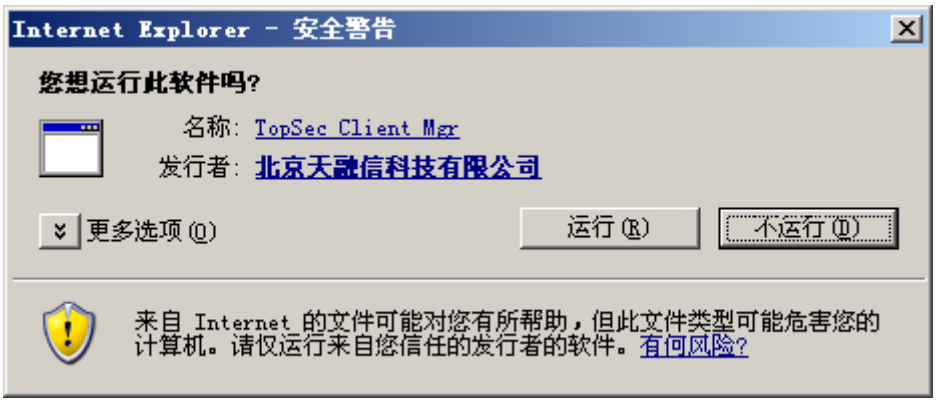
如果管理员配置的控件安装方式为“手动安装”，则用户成功登录网关后，网关将弹出如下界面，提示用户手动安装“天融信下载管理控件”。



点击“这里”链接，弹出“文件下载”对话框，如下图所示。



点击“保存”按钮，可以将“天融信下载管理控件”的安装程序保存到本地，以便后续手动安装，但是，此时的用户端没有安装任何控件和组件，所以用户将无法访问任何资源。点击“运行”按钮，弹出运行该软件的安全警告对话框，如下图所示。

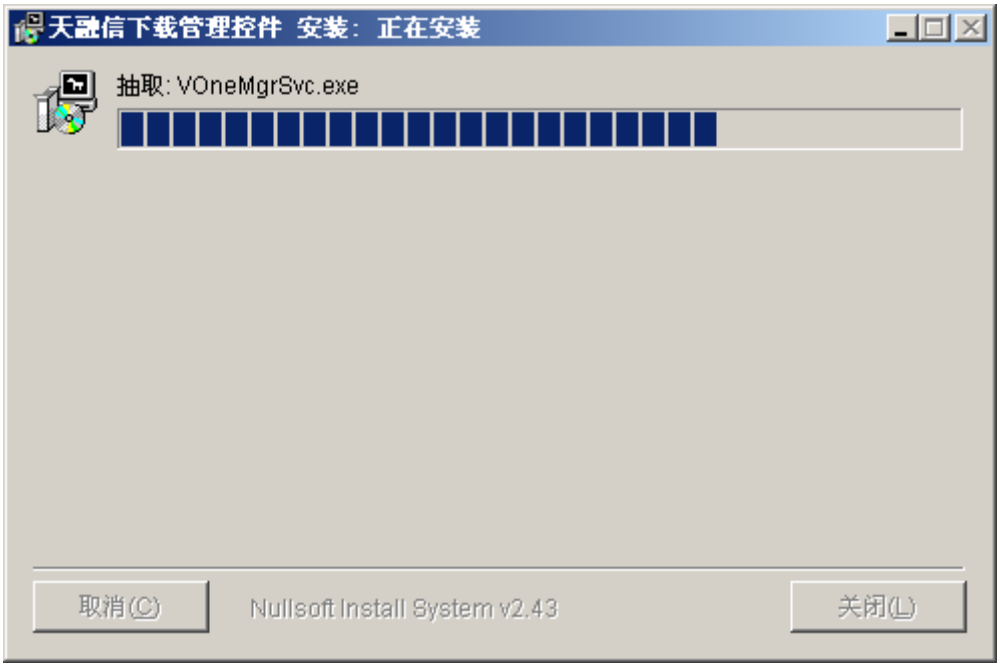


点击“运行”按钮，开始安装“天融信下载管理控件”，进入步骤 2）。

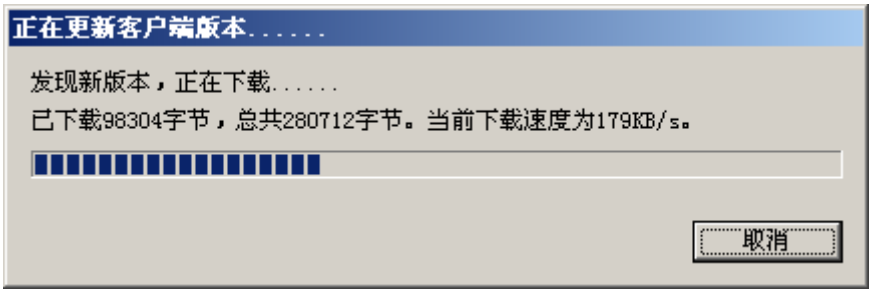
说明

- ✧ 用户登录前必须安装“天融信下载管理控件”，否则无法安装其他任何组件，同时无法登录并访问内网资源。
- ✧ 如果由于用户主机的安全级别设置较高而导致不允许用户安装“天融信下载管理控件”，登录界面会禁止用户登录。用户可以根据界面提示信息修改安全级别，然后重新打开浏览器进行连接即可。

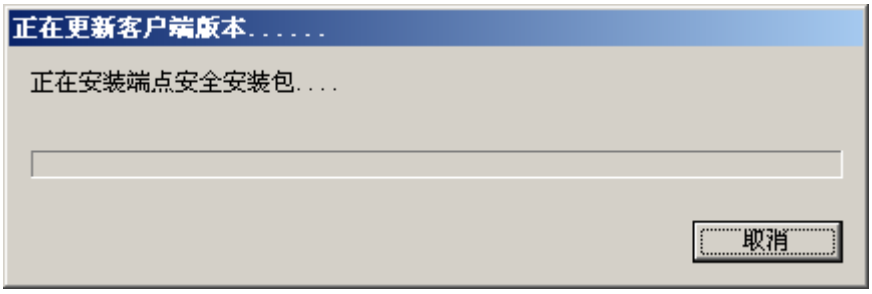
2）在自动安装方式下点击“安装”按钮，或者在手动安装方式下点击“运行”按钮后，开始在用户系统中安装“天融信下载管理控件”，如下图所示。



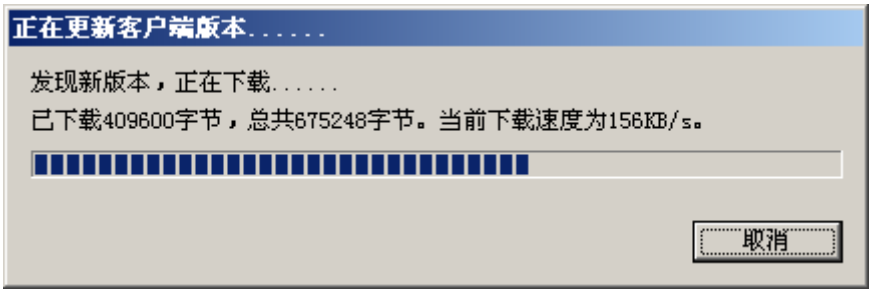
3）控件安装完成后，开始下载端点安全组件的安装程序，如下图所示。



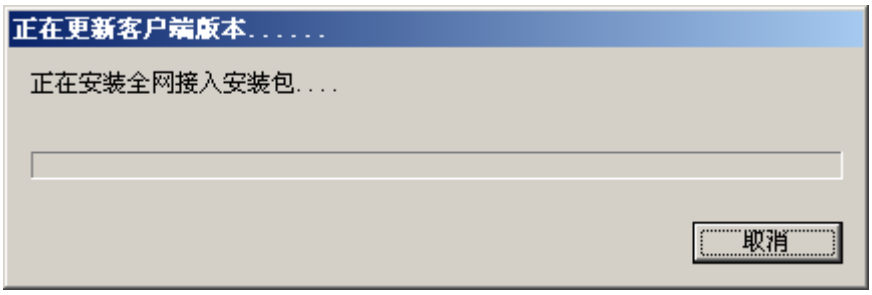
4）下载完成后，开始安装端点安全组件，如下图所示。



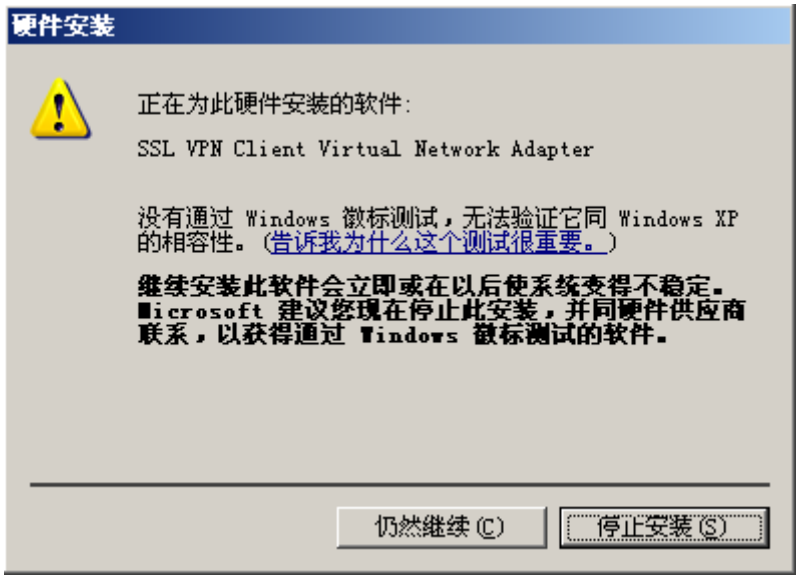
5）端点安全组件安装完成后，开始下载全网接入组件的安装程序，如下图所示。



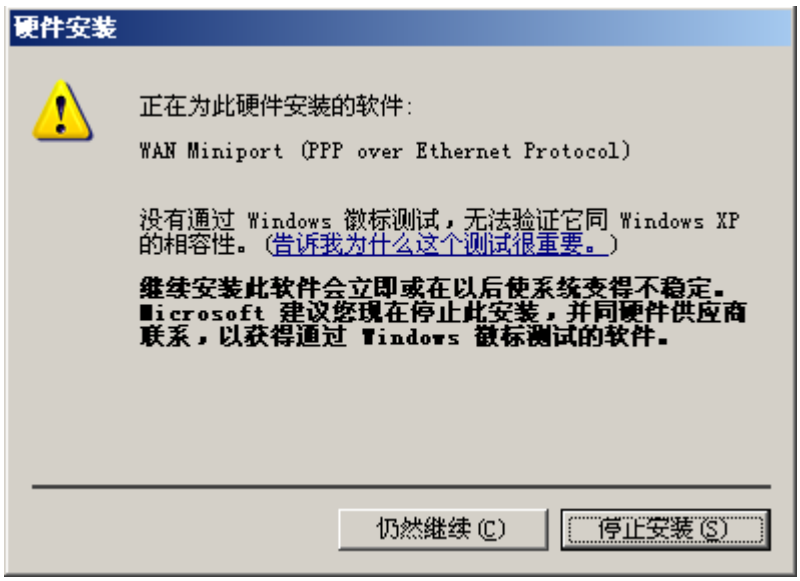
6）下载完成后，开始安装全网接入组件，如下图所示。



提示用户安装虚拟网卡，如下图所示。

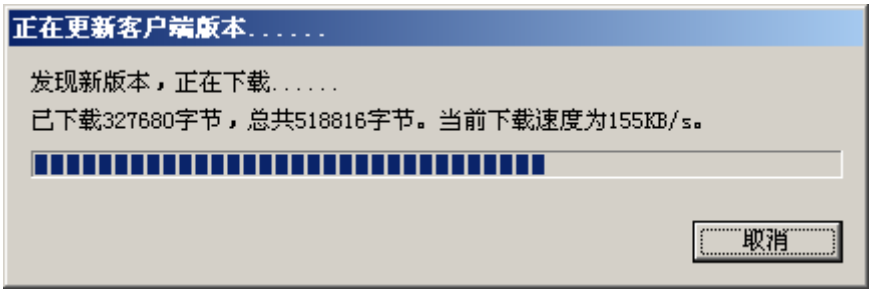


点击“仍然继续”按钮，安装完成后，提示用户安装 WAN Miniport，如下图所示。

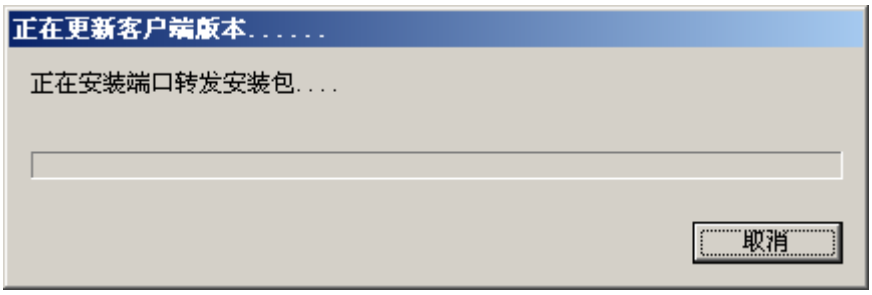


点击“仍然继续”按钮，继续安装。

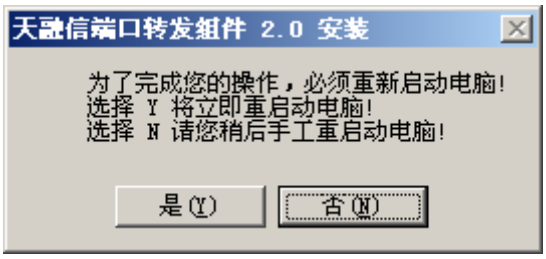
7）全网接入组件安装完成后，开始下载端口转发组件的安装程序，如下图所示。



8）下载完成后，开始安装端口转发组件，如下图所示。



9）端口转发组件安装完成后，提示用户重启电脑，如下图所示。



10）点击“是”按钮，立刻重新启动电脑；点击“否”按钮，稍后重启电脑。建议用户安装完所有控件和组件后，重启客户端主机。

说明

- ✧ 用户每次登录前，网关都会检查用户系统中安装的控件和组件是否是最新版本，如果不是最新版本，则提示用户下载安装。

3.1.2 退出网关

用户结束授权资源的访问之后，为了安全起见，建议立即断开与 SSLVPN 网关的连接。一般情况下，用户与网关断开连接的方式有四种：（1）注销会话；（2）关闭浏览器；（3）用户超时；（4）被管理员强制退出。

1．注销会话。

用户在注销会话后，界面退回到登录界面，SV 客户端托盘断开连接，并且客户端的端点安全控件自动为用户清理主机上残留的各种不安全的缓存信息，同时 SSL VPN 网关删除该用户的会话信息。对于用户来说，“注销”是一种便捷并且安全的退出方式，其具体操作如下所示：

1）在用户界面中，点击 LOGO 图片右侧的“注销”链接，弹出注销确认框，如下图所示。

2）点击“确定”按钮即可安全退出用户界面。

2．关闭浏览器。

如果用户没有通过“注销”链接退出用户界面，而只是关闭了用户浏览器，那么用户屏幕下方的“SV 客户端”托盘不会断开，以致于该用户后续虽然无法再访问 WEB 转发资源和应用 WEB 化资源，但是仍然可以通过端口转发客户端和全网接入客户端访问相应资源，同时 SSL VPN 网关中仍然保存了该用户的会话信息。

综上所述，对于用户来说，仅仅关闭浏览器并不是一种安全的退出方式，还需要断开“SV 客户端”托盘：右键单击“SV 客户端”托盘，然后点击菜单项“断开”；或者单击“SV 客户端”托盘，然后点击“断开”按钮。

说明

- ✧ 用户在进行正常的内网访问时，不要关闭主页面，主页面一旦被关闭或者退出，用户后续对于“WEB 转发”资源和“应用 WEB 化”资源的访问将被拒绝。

3．用户超时。

如果用户在管理员设定的超时时间内没有任何资源访问动作，那么在超时时间之后用户所做的任何访问请求将被拒绝，同时弹出错误提示界面，然后跳转到用户登录界面，提示用户重新登录。用户超时后，可以重新登录网关。

4．被管理员强制退出。

管理员在 SSL VPN 网关中删除某个用户的会话后，网关将拒绝用户所做的任何访问请求，同时弹出用户登录界面，提示用户重新登录。用户被管理员强制退出后，可以重新登录网关。

3.2介绍用户主界面

根据网关管理员配置的虚拟门户，用户登录成功并正确安装天融信下载管理控件和所有组件后，弹出的用户界面可能会出现以下三种情况：（1）只弹出用户主界面，其显示内容和显示风格由网关管理员进行配置；（2）只弹出企业门户网站，其显示内容和显示风格由部署该网关的企业进行配置；（3）弹出企业门户网站，同时保留用户主界面，用户可以在两个页面之间自由切换。由于企业门户网站千差万别，所以如无特殊说明，本文档只描述用户主界面的操作。

下面以 IE6.0 用户主界面为例进行介绍，如下图所示。

整个主界面分为四大部分，下面分别进行详细描述：

1）页面最上方显示了 SSL VPN 网关当前的 LOGO 图片，管理员可以为不同的门户配置不同风格的 LOGO 图片，因此用户登录不同的门户可能会看到不同的 LOGO。

LOGO图片的右侧显示了登录的用户名称，以及用户界面的辅助功能，包括：“帮助”链接、“注销”链接、“设置风格”链接和“修改密码”链接。单击“帮助”链接可以查看用户界面的帮助信息；单击“注销”链接，可以退回到用户登录界面，同时关闭用户屏幕底部的“SSL VPN客户端”托盘，具体请参见 3.1.2退出网关 的相关介绍；单击“设置风格”链接，可以设置用户登录页面风格和主页面风格，具体请参见 3.3设置页面风格 的相关介绍；单击“修改密码”链接，可以修改该用户自己的密码，具体请参见 3.4修改用户密码 的相关介绍。

说明

- ✧ 如果页面中显示的用户名称以“...”结尾，说明该用户名称太长而无法全部显示。此时，

只需将鼠标置于用户名上即可显示完整的用户名称。

2）LOGO 图片的正下方显示了管理员配置的自定义页面信息，如上图为“天融信 SSLVPN 网关用户界面！”。

3）自定义页面信息的左下方显示了管理员配置的公告信息，如上图为“欢迎使用天融信 SSL VPN 网关！”，点击该栏右侧的“×”按钮可以关闭该公告信息。

4）主界面的主体部分包括三个页签内容，“资源列表”页签中显示了管理员授权用户访问的资源列表，具体请参见 3.5访问内网资源 的相关介绍；“配置”页签中显示了用户需要自行配置的一些基本内容，包括客户端日志和WEB SSO，具体请参见 3.6配置WEB SSO和日志级别；“状态”页签中显示了SSL VPN客户端的状态（即：全网接入和端口转发）以及用户的登录信息，具体请参见 3.7查看和配置客户端状态。

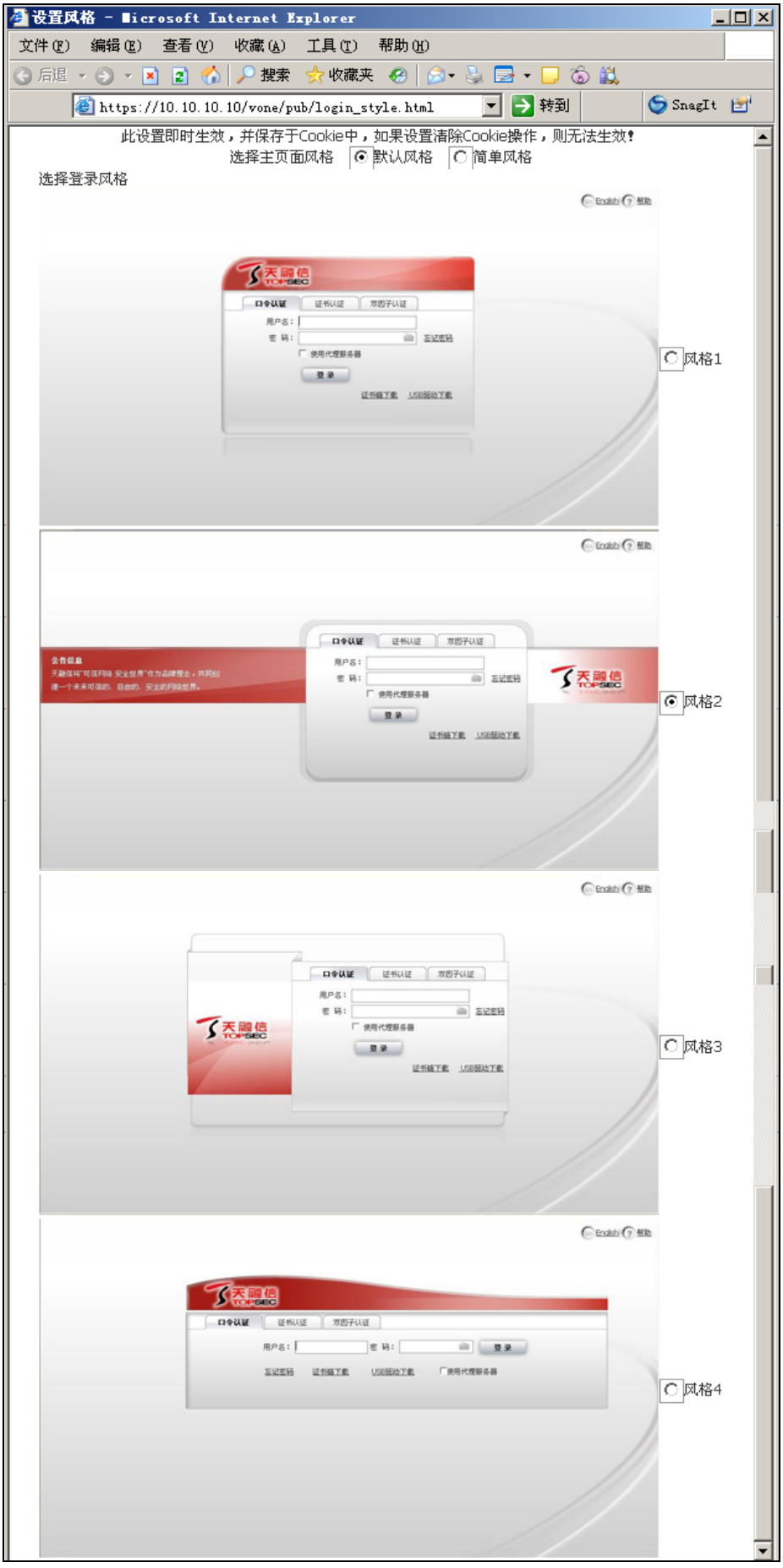
说明

- 用户在进行正常的内网访问时，不要关闭或退出主页面，主页面一旦被关闭或者退出，远程用户与 VPN 网关之间的 SSL 隧道连接将自动清除，用户后续的访问将被拒绝。
- 如果用户在管理员设定的超时时间内没有任何资源访问动作，那么在超时时间之后用户所做的任何访问请求将被拒绝，并跳转到超时提示界面提示用户，用户需要重新登录网关。

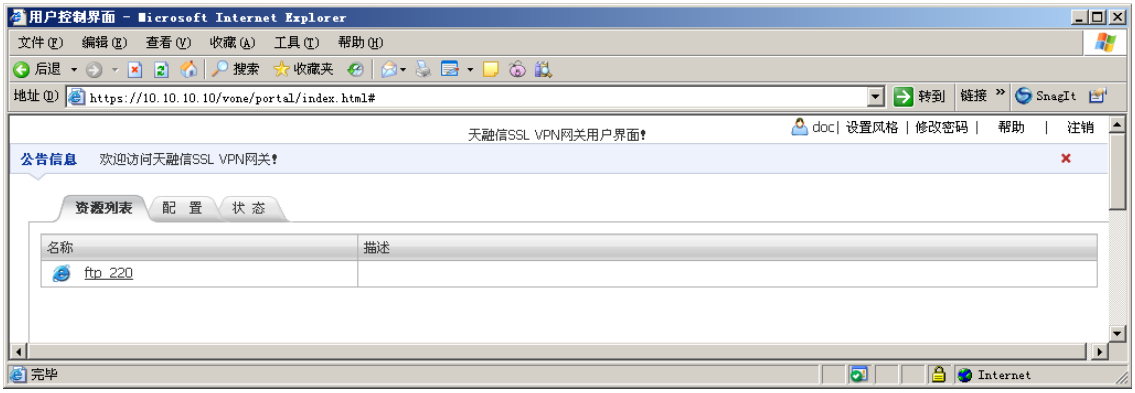
3.3设置页面风格

用户可以在当前主机中自定义用户登录页面风格和用户主页面风格，当该用户下次使用该主机进行登录时，将应用最新定义的登录风格和主页面风格。用户自定义页面风格的具体操作如下所示：

1）用户成功登录网关并进入用户界面后，点击 LOGO 图片右侧的“设置风格”，进入“设置风格”页面，如下图所示。


设置风格 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
https://10.10.10.10/vone/pub/login_style.html
转到
SnagIt
此设置即时生效，并保存于Cookie中，如果设置清除Cookie操作，则无法生效!
选择主页面风格 默认风格 简单风格
选择登录风格
风格1
风格2
风格3
风格4

2）在“选择主页面风格”右侧，选中“默认风格”或“简单风格”。“默认风格”是指 SSL VPN 网关的虚拟门户中定义的主页面风格；“简单风格”定义的主页面风格如下图所示。



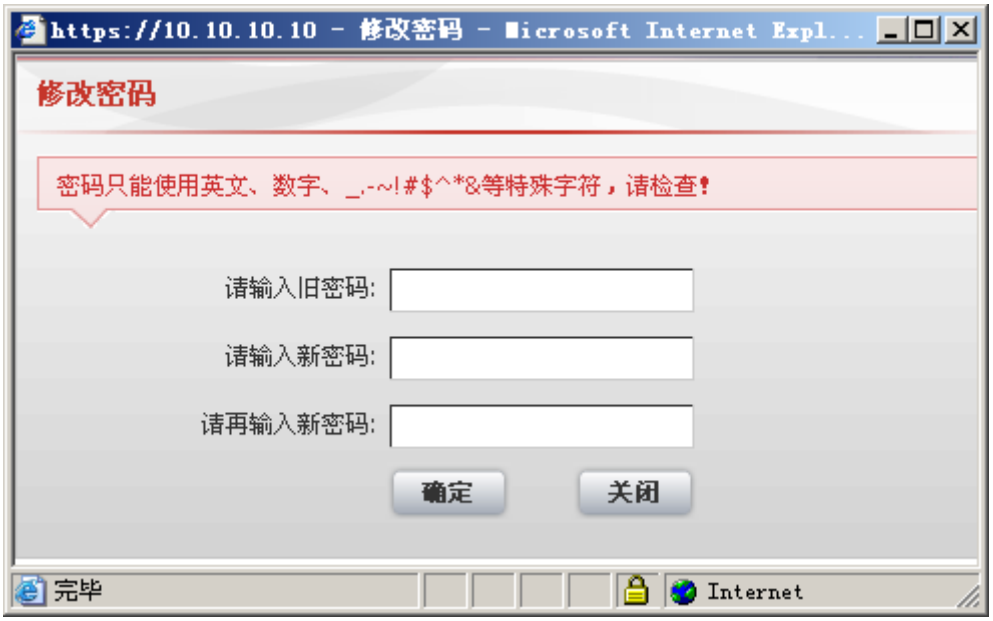
3）在“选择登录风格”下方，选中某个登录风格。

4）页面风格选择完成后，点击窗口右上方的关闭按钮“”即可完成配置，当用户下次使用该主机进行登录时，将应用最新定义的登录风格和主页面风格。

3.4修改用户密码

为了防止密码泄露带来的不安全因素，用户登录 SSL VPN 网关后，可以自行修改用户密码，具体操作步骤如下所示：

1）用户成功登录网关并进入用户界面后，点击 LOGO 图片右侧的“修改密码”，进入“修改密码”页面，如下图所示。



2）输入该用户的旧密码，然后设置新密码。

3）参数设置完成后，点击“确认”按钮，完成用户密码的修改操作。

3.5访问内网资源

SSL VPN 网关支持远程用户以多种方式访问内网资源，包括：WEB 转发，端口转发，全网接入和应用 WEB 化。需要注意的是：（1）用户的授权资源，以及用户访问授权资源的方式由网关管理员的配置所决定；（2）目前，天融信 SSL VPN 网关不支持网关管理员为用户同时开启端口转发方式和全网接入方式。因此，远程用户如果需要更改权限和访问方式，必须联系管理员进行相应的配置。

基于管理员在管理界面的配置，主页面的资源列表中只显示了用户有权访问，并且允许显示在页面中的资源。对于显示在资源列表中的授权资源，用户可以直接点击资源列表中的资源名称，系统会自动启动网页浏览器或相关联的客户端应用程序来访问资源；而对于未能显示在资源列表中的授权资源，用户只能手动打开一个网页浏览器或客户端应用程序进行资源访问。下面主要介绍如何访问或操作不同类型的内网资源。

说明

- ✧ 只有管理员为用户启动了某些功能模块，用户才能够使用相应模块访问授权资源。

3.5.1Web 转发

用户成功登录网关后，无需安装任何客户端组件，就可通过 WEB 转发方式安全的访问公司内部 B/S 结构应用。管理员已经建立了内部 Web 转发的 HTTP 代理，并授权给用户，用户登录进入主页面后，访问 web 转发资源的步骤如下所示：

1）在用户主页面中，激活“资源列表”页签。

2）对于授权用户访问并且允许显示在用户界面中的 web 转发资源，点击某个 web 转发资源的名称（如下图中的“wf_235”），即可访问授权页面。

资源列表由管理员设置，用户不能对其进行添加、删除和修改操作。

说明

- ✧ web 转发资源在管理员进行配置时，强制在授权用户界面上显示，没有在资源列表里的内网资源，无法通过 web 转发访问。

3.5.2 端口转发

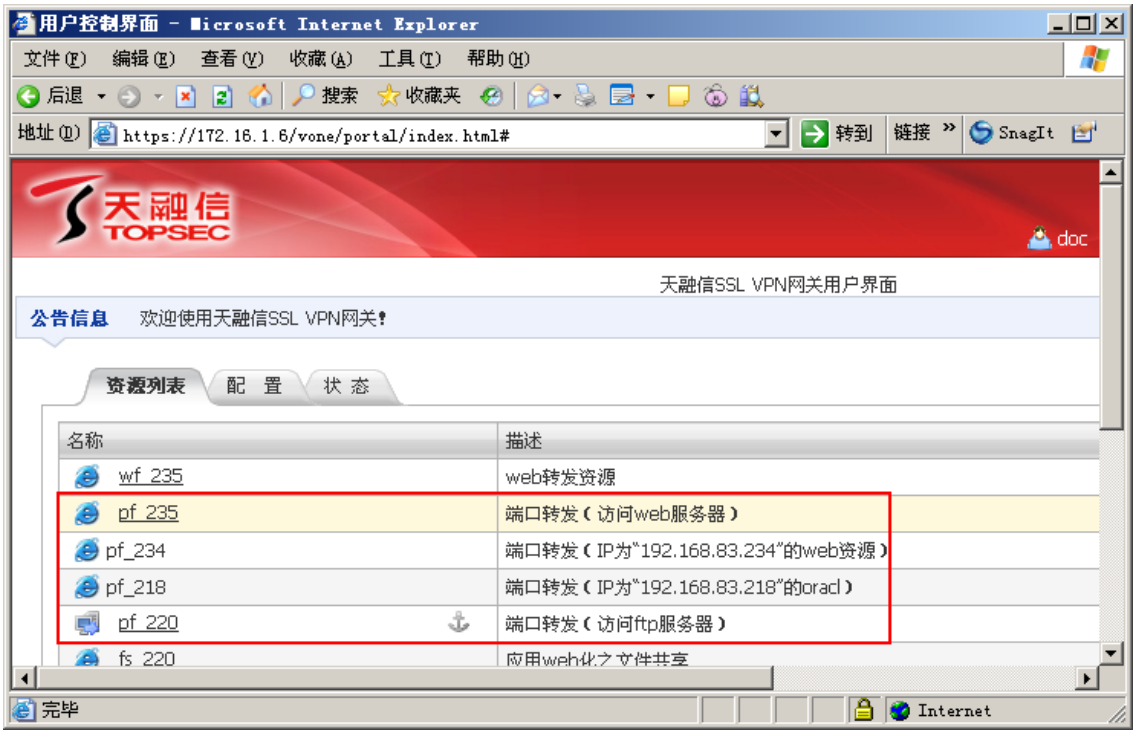
只有正确安装并加载了端口转发组件后，用户才能通过端口转发模块访问内部网络资源。用户登录进入主页面后，访问端口转发资源的步骤如下所示：

1）激活“状态”页签，然后点击“端口转发状态”右侧的“启动”链接，以便启用端口转发客户端，如下图所示。

说明

- ✧ 目前，天融信 SSL VPN 网关不支持网关管理员为用户同时开启端口转发模块和全网接入模块，所以用户不能同时启动端口转发客户端和全网接入客户端。

2）待端口转发客户端正常运行后，对于授权用户访问并且允许显示在用户界面中的端口转发资源，可以在“资源列表”页签中查看，如下图所示。



a）当图标为“ ”，并且资源名称下方有下划线（如上图中的“pf_235”）时，表示该端口转发资源可以用网页浏览器打开。此时，点击资源名称后，可以自动打开网页浏览器进行访问。

b）当图标为“ ”，但是资源名称下方没有下划线（如上图中的“pf_234”和“pf_218”）时，表示网关管理员添加该端口转发资源时没有配置“资源地址”。此时，用户可以联系网关管理员获取该资源服务器的类型和地址，然后打开网页浏览器或者 C/S 客户端应用程序进行访问。

c）当图标为“ ”，并且资源名称下方有下划线（如上图中的“pf_220”）时，表示该端口转发资源可以使用某个 C/S 客户端应用程序打开。此时，用户需要先点击该资源右侧的图标“ ”或者该资源名称，选择访问该资源的 C/S 客户端应用程序，然后再点击资源名称，将自动打开选择的 C/S 客户端应用程序，以便用户访问授权资源。

说明

- 如果网关管理员在配置端口转发资源时已经定义了必须使用哪个 C/S 客户端应用程序访问资源服务器，则该用户必须使用相应的 C/S 客户端应用程序访问授权资源，否则访问被禁止。

3）待端口转发客户端正常运行后，对于授权用户访问但是并没有显示在用户界面中的端口转发资源，用户可以联系网关管理员获取授权资源服务器的类型和地址，然后打开网页浏览器或者 C/S 客户端应用程序进行访问。

用户访问端口转发资源的过程中，必须保持端口转发客户端和网关的正常连接，否则访问中断。“端口转发”资源由管理员设置，用户不能对其进行添加、删除和修改操作。

3.5.3 全网接入

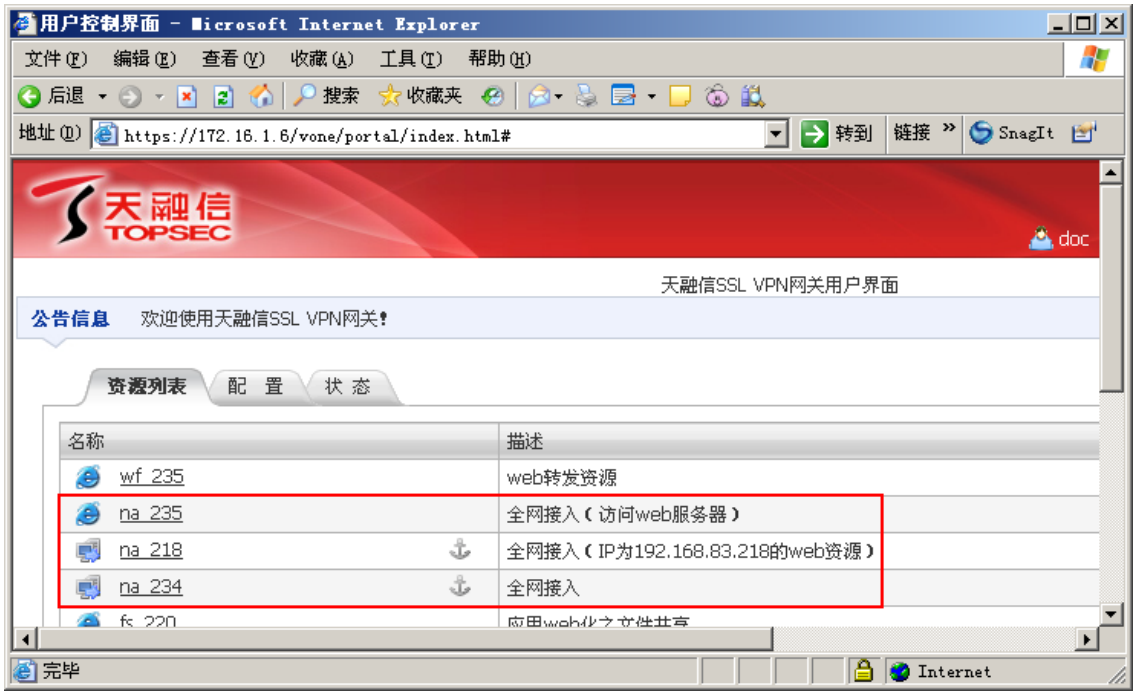
只有正确安装并加载了全网接入组件后，用户才能通过全网接入模块访问内网中被授权的 B/S 和 C/S 应用。用户登录进入主页面后，访问全网接入资源的步骤如下所示：

1）激活“状态”页签，然后点击“全网接入状态”右侧的“启动”链接，以便启用全网接入客户端，SSL VPN 隧道成功建立后的界面如下图所示。

说明

- ✧ 目前，天融信 SSL VPN 网关不支持网关管理员为用户同时开启端口转发模块和全网接入模块，所以用户不能同时启动端口转发客户端和全网接入客户端。

2）待 SSL VPN 隧道建立成功后，对于授权用户访问并且允许显示在用户界面中的全网接入资源，可以在“资源列表”页签中查看，如下图所示。



a）当图标为“ ”时，表示该全网接入资源可以用网页浏览器打开。此时，点击资源名称后，可以自动打开网页浏览器进行访问。

b）当图标为“ ”时，用户可以联系网关管理员获取该资源服务器的类型和地址，然后打开网页浏览器进行访问，或者点击图标“ ”选择 C/S 客户端应用程序后，再点击资源名称，以便自动打开选择的 C/S 客户端应用程序访问授权资源。

3）待 SSL VPN 隧道建立成功后，对于授权用户访问但是并没有显示在用户界面中的全网接入资源，用户可以联系网关管理员获取授权资源服务器的类型和地址，然后打开网页浏览器或者 C/S 客户端应用程序进行访问。

用户访问全网接入资源的过程中，必须保持全网接入客户端和网关的正常连接，否则访问中断。“全网接入”资源由管理员设置，用户不能对其进行添加、删除和修改操作。

3.5.4 应用 WEB 化

用户登录后无需安装任何客户端控件，即可使用应用 WEB 化功能，通过 SSL 安全地访问企业内部文件共享服务器。用户登录进入主页面后，访问应用 web 化资源的步骤如下所示：

1）在用户主页面中，激活“资源列表”页签，可以查看授权用户访问的应用 web 化资源，如下图所示。

根据网关管理员的配置，用户可以使用“文件共享”或者“ftp 服务器”方式访问“应用 web 化”资源。“文件共享”方式指通过网上邻居的方式访问该服务器的文件共享资源；“ftp 服务器”方式指通过 FTP 协议方式访问该服务器的 FTP 服务器资源。

“应用 WEB 化”资源由管理员设置，用户不能对其进行添加、删除和修改操作。

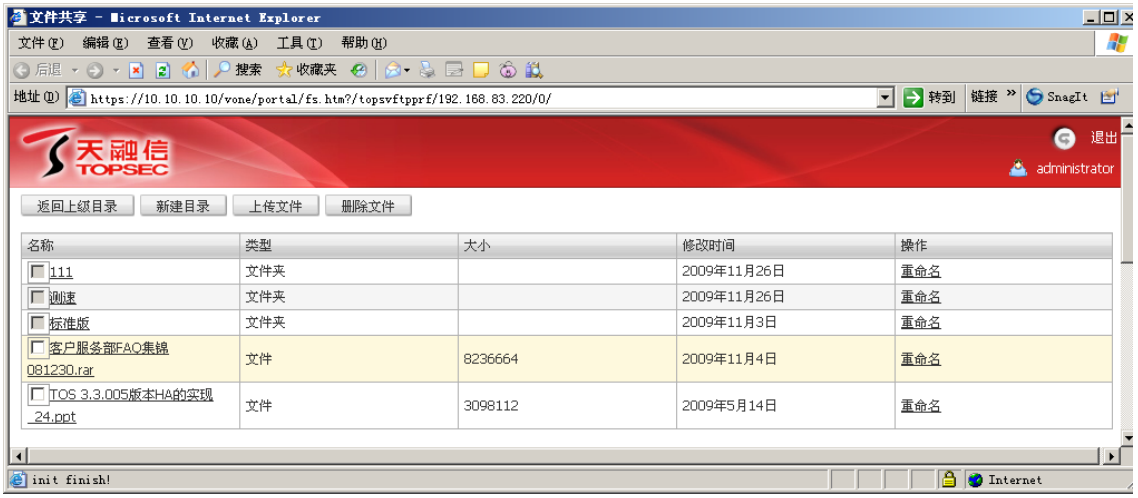
2）对于授权用户访问并且允许显示在用户界面中的应用 web 化资源，用户可以点击某个应用 web 化资源的名称，然后进入文件共享服务器或 ftp 服务器的登录页面。

3）对于授权用户访问但是并没有显示在用户界面中的应用 web 化资源，用户可以打开网页浏览器，然后在地址输入框中输入授权的资源服务器 URL（如：ftp://192.168.100.18），进入文件共享服务器或 ftp 服务器的登录页面。

用户通过 FTP 方式和文件共享方式访问应用 web 化资源的操作类似，下面以 FTP 方式访问应用 WEB 化资源“ftp_220_ftp”为例，详细介绍各操作：

1）在用户主页面中，激活“资源列表”页签，然后点击应用 web 化资源名称“fs_220_ftp”。如果用户在当前登录中第一次访问该 FTP 服务器，则首先进入其登录界面，如下图所示。

2）根据 FTP 服务器的相关配置，输入 FTP 服务器的用户名和密码或者选中“匿名登录”，然后点击“登录”按钮，界面中显示 FTP 服务器中根目录下的所有共享文件/文件夹，如下图所示。



3）点击根目录下的文件夹名称，如果该文件夹允许所有用户访问，则界面中将显示该文件夹下的共享内容；否则，将跳转到认证页面，需要输入该文件夹允许的用户名和密码才能够查看或编辑其中的内容，如下图所示。

说明

- ✧ 用户对内网共享文件的操作权限取决于两个因素：首先管理员在 VPN 网关上为用户指定的访问控制规则，其次是文件共享主机上对用户的访问权限控制。在上述的授权控制下，用户可以对共享文件和文件夹进行添加、删除、重命名等操作。

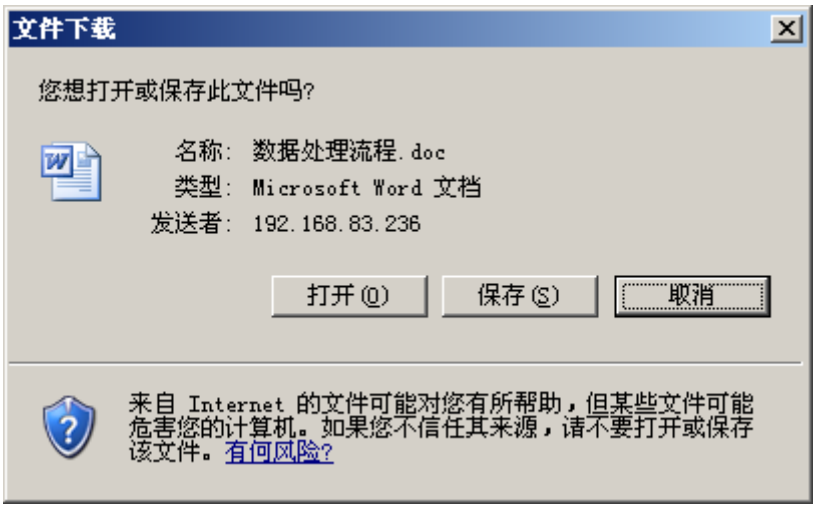
4）输入该文件夹允许访问的用户名和密码后，可以查看或编辑该文件夹中的内容，如下图所示。

界面中从上往下依次为：（1）SSL VPN 网关的 LOGO 图片（由管理员设定）；（2）访问该文件夹的用户名称和“退出”操作链接；（3）各种操作的链接，包括返回上级目录、新建目录、上传文件、删除文件；（4）显示该文件夹下的内容，包括文件或文件夹的名称、类型（文件或文件夹）、文件大小、修改时间和“重命名”操作链接。

下面分类介绍一下用户的各种操作(假设管理员设定的安全策略和文件共享服务器上的共享权限均允许用户进行所有操作)，包括 查看/下载文件、返回上级目录、新建目录、上传文件、删除文件、修改文件/文件夹的名称、删除空目录 和 退出文件共享服务器的访问页面 查看/下载文件 查看/下载文件。

a）查看/下载文件。

① 点击待查看/下载的文件名称，弹出“文件下载”对话框，如下图所示。



② 点击“打开”按钮，可以浏览该文件；点击“保存”按钮，然后选择保存路径，可以将该文件保存到本地。

b）返回上级目录。

点击“返回上级目录”链接，可以返回上一级文件夹。

c）新建目录。

① 点击“新建目录”链接，可以在当前目录下添加新目录，如下图所示。

② 输入新建目录名称。

③ 点击“提交”按钮即可。

d）上传文件。

① 点击“上传文件”链接，可以在当前目录下添加文件，如下图所示。

② 在“上传文件[最大支持 150M]路径”中填写希望上传的文件存储路径；或者点击“浏览…”按钮进行查找。

③ 选择遇到相同文件名的处理方法，覆盖或跳过。

“覆盖”指上传的同名文件替换掉服务器中的文件；“跳过”指保留服务器中的文件，丢弃上传的同名文件。

④ 点击“提交”按钮后，在文件处理过程中，可以点击“取消操作”按钮取消此次上传操作，如下图所示；否则将成功完成文件上传。

e）删除文件。

① 勾选待删除文件前的复选框。

② 点击“删除文件”链接即可。

f）修改文件/文件夹的名称。

① 点击待修改文件/文件夹条目的“重命名”链接，文件/文件夹的名称将会显示为可修改状态，如下图所示。

② 修改文件/文件夹名称后，鼠标点击任意处即可。

g）删除空目录。

当目录中没有文件时，操作链接一行如下图所示。

点击“删除空目录”链接后，当前空目录被删除，页面跳转到上一级目录内容。

说明

- ✧ 对于共享文件不允许的操作，用户界面中将会弹出提示信息“禁止操作!您没有权限访问此页面”或“Permission denied”。
- ✧ 对于网关的 ACL 不允许的操作，用户界面将会弹出提示信息“ACL 禁止操作”。

h）退出文件共享服务器的访问页面。

在文件共享服务器的任意目录下，点击页面右上方的“退出”链接，可以成功退出该文件共享服务器的访问页面。

3.6配置 WEB SSO 和日志级别

WEB SSO（Web Single Sign-On，Web 单点登录）是天融信 SSL VPN 网关为 HTTP 和 HTTPS 服务提供的单点登录的扩展功能。

管理员可以将资源服务器的“用户名”和“密码”之外的其它登录参数配置到管理员界面的 WEB SSO 配置中，然后在用户 SSL VPN 登录网关后，通过 WEB SSO 配置页面添加登录该服务器的用户名和密码，最后将其同步到服务器，以便在用户访问后台 WEB 服务器时自动输入该登录信息进行身份认证，无须用户手工输入用户名和密码。在网关中配置 WEB SSO 的具体操作请参见《NGFW 管理手册——SSL VPN 配置》的详细描述，在客户端实现 WEB SSO 的具体步骤如下所示：

1)管理员在网关中为资源 A 配置 WEB SSO 的单点登录方式。具体步骤请参见《NGFW 管理手册——SSL VPN 配置》的相关介绍。

2）用户登录 SSL VPN 网关。

3）用户在客户端为资源 A 配置 WEB SSO 相关参数，即访问资源 A 时需要提供的用户名和密码。步骤 3）是可选配置，如果访问资源 A 的用户名和密码与登录 SSL VPN 网关的用户名和密码一致，则无须配置步骤 3）；否则，必须配置步骤 3）。具体操作如下所示：

a）在用户界面中，激活“配置”页签，如下图所示。

b）添加 WEB SSO 登录信息。

在“WEB SSO 配置”一栏，点击“添加”配置 WEB SSO 登录信息，如下图所示。

界面参数如下表所示。

参数	说明
资源名称	允许单点登录的资源的名称。 说明： 该资源服务器必须是使用了“HTTP 基本验证”的 Web 服务器，这些 Web 服务器要求访问者在浏览网站之前输入用户名和密码，从而获得保护。
SSO 用户名	登录该资源的用户名称。
SSO 密码	登录该资源的用户密码。

参数设置完成后，点击“同步服务器”按钮，将配置保存到 SSL VPN 网关中。

c）删除 WEB SSO 登录信息。

在“WEB SSO 配置”一栏，点击待删除的配置条目右侧的“动作”按钮，即可删除该条目。

然后点击“同步服务器”按钮，将该操作同步到 SSL VPN 网关中。

d）清空 WEB SSO 登录信息。

在“WEB SSO 配置”一栏，点击“清空”即可清空 WEB SSO 配置列表。

然后点击“同步服务器”按钮，将该操作同步到 SSL VPN 网关中。

说明

- “日志设置”一栏中，端口转发日志级别和全网接入日志级别的设置主要用于开发、维护人员定位问题，用户无需关注。

3.7查看和配置客户端状态

用户可以查看全网接入和端口转发的客户端状态，启用/关闭全网接入或端口转发模块，查看该用户登录 SSL VPN 网关的一些基本信息。需要注意的是：目前，天融信 SSL VPN 网关不支持网关管理员为用户同时开启端口转发模块和全网接入模块，所以用户不能同时启动端口转发客户端和全网接入客户端。

查看以及配置客户端状态的的具体操作如下所示：

1）在用户界面中，点击“状态”页签，如下图所示。

2）查看全网接入客户端的状态。

在“全网接入状态”一栏，用户可以查看 SSL VPN 隧道建立过程中的状态变化，传输流量、隧道连接方式、连接时间、虚拟网卡的相关信息。

说明

- “连接方式”由管理员设定，决定用户可访问资源。若“连接方式”为“网络隔离”，表明用户端设备完全作为内网设备，远程主机的默认网关设置为虚拟网卡 IP，则原来需要经过默认网关转发的应用都要经过 SSL VPN 网关；若“连接方式”为“透明访问”，表明用户访问访问内网资源时通过网关转发，不影响用户访问原有的外网资源。

3）启动/关闭全网接入功能。

全网接入模块的启动方式由管理员设置。如果管理员设置为自动运行，则用户登录后进入主界面后全网接入控件将自行启动并完成 SSL 隧道的协商过程。如果管理员设置为手动运行，则需要用户手动开启全网接入功能。

用户可以点击“全网接入状态”一栏中的“启动”，启动全网接入模块，建立与网关设备的 SSL VPN 隧道；或者点击“关闭”，中断全网接入。

说明

- ✧ 如果管理员开启了自动重连功能，则当全网接入服务异常中断后，可以自动地连续重连。但是当用户点击“停止”主动停止全网接入功能时，全网接入服务将不会进行重连。
- ✧ 只有当网关管理员为用户开启了全网接入模块，该用户才能够启动全网接入客户端。

4）查看端口转发客户端的状态。

在“端口转发状态”一栏，用户可以查看端口转发组件的运行状态，传输流量以及连接时间等相关信息。

5）关闭/启动端口转发功能。

端口转发模块默认为启动状态，用户可以点击“端口转发状态”一栏中的“关闭”，中断端口转发；或者点击“启动”，启动端口转发模块。

说明

- ✧ 只有当网关管理员为用户开启了端口转发模块，该用户才能够启动端口转发客户端。

6）查看该用户的登录信息。

在“登录信息”一栏，用户可以查看自己本次登录成功 IP/时间，上次登录成功 IP/时间，以及上次登录失败 IP/时间。

4使用独立客户端

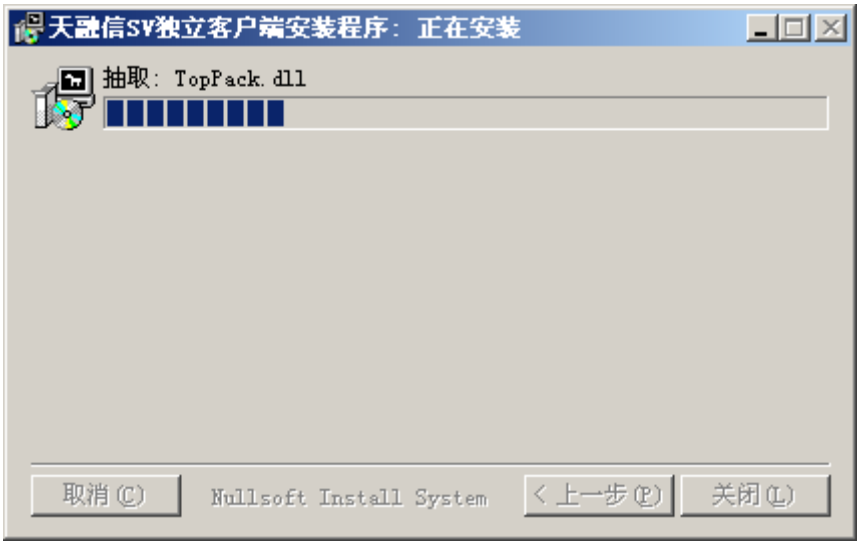
SSL VPN用户使用客户端主机登录天融信SSL VPN网关的方式包括两种：（1）基于B/S架构，使用网页浏览器登录天融信SSL VPN网关，然后访问授权资源，具体操作请参见 3使用网页浏览器 的相关介绍；（2）基于C/S架构，安装并运行“天融信SV独立客户端”，然后登录网关并访问授权资源，具体操作请参见本章的相关介绍。

天融信公司在随机光盘中附送了 SSL VPN 独立客户端的安装程序“SVClientSetup.exe”，用户可向网关管理员索取。下面主要介绍独立客户端的安装和使用：

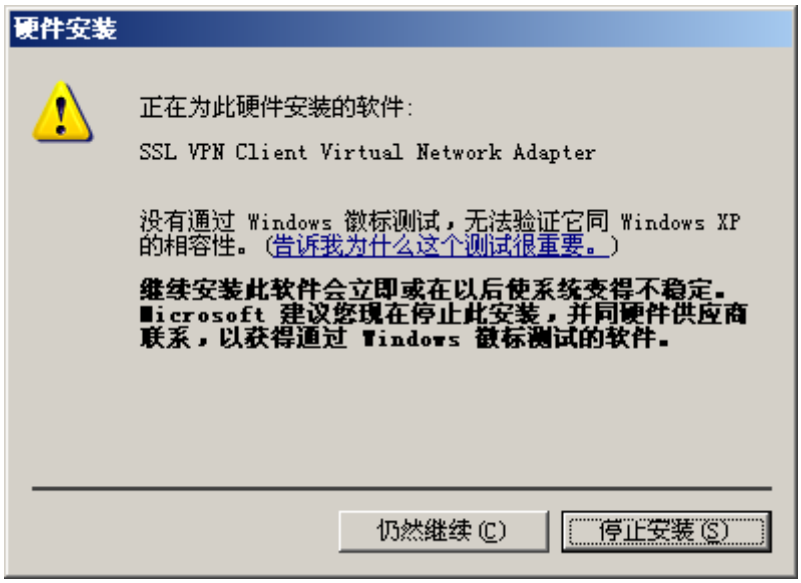
1．安装 SSL VPN 独立客户端。

a）运行“SVClientSetup.exe”后，弹出对话框，提示用户选择“天融信 SV 独立客户端”的安装路径，如下图所示。

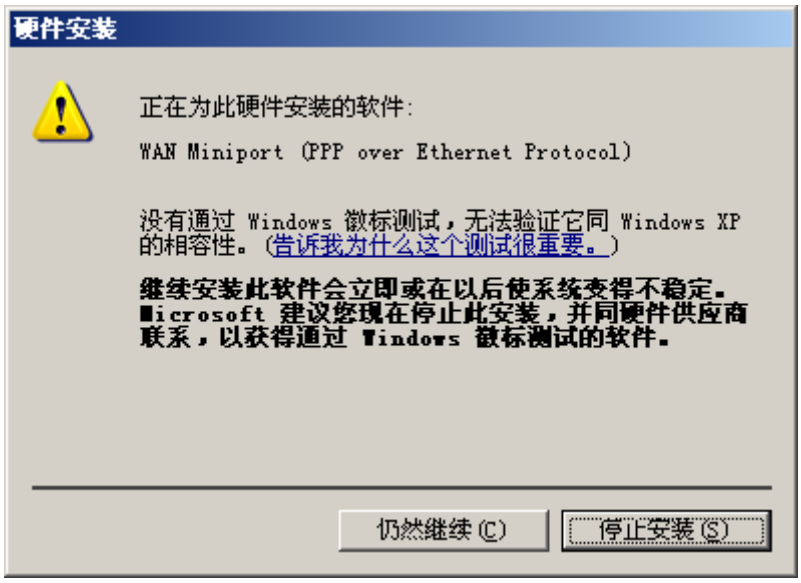
b）点击“浏览”按钮可以更改安装路径。安装路径设置完成后，点击“安装”按钮，开始安装天融信 SV 独立客户端，如下图所示。



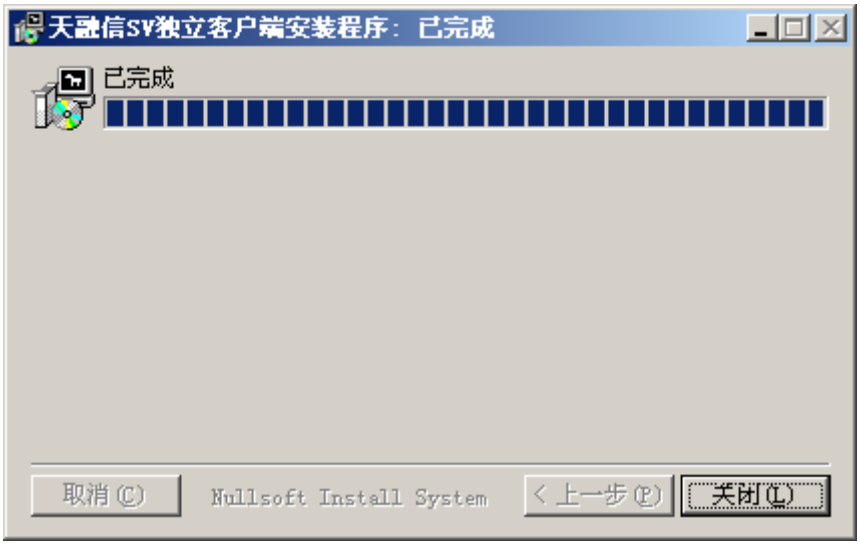
c）安装过程中，提示用户安装虚拟网卡，如下图所示。



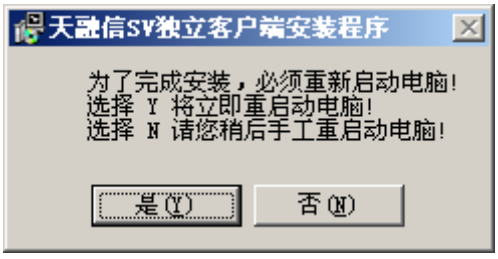
d）点击“仍然继续”按钮，虚拟网卡安装完成后，提示用户安装 WAN Miniport，如下图所示。



e）点击“仍然继续”按钮，继续安装，稍候，提示用户已经完成“天融信 SV 独立客户端”的安装，如下图所示。



f）点击“关闭”按钮，弹出提示框，提示用户重新启动电脑，如下图所示。

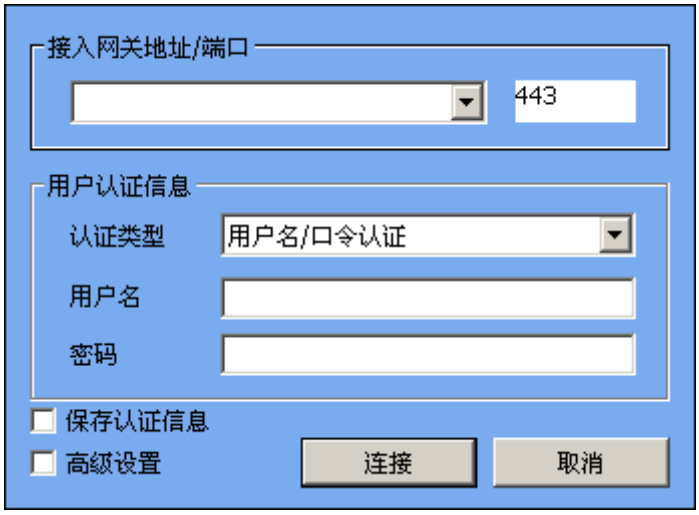


g）选择“是”重启电脑；选择“否”，可以稍后手工重启电脑。建议用户重启电脑后再登录 SSL VPN 网关访问授权资源。

2．使用 SSL VPN 独立客户端登录网关。

a）双击用户主机桌面上的快捷图标“

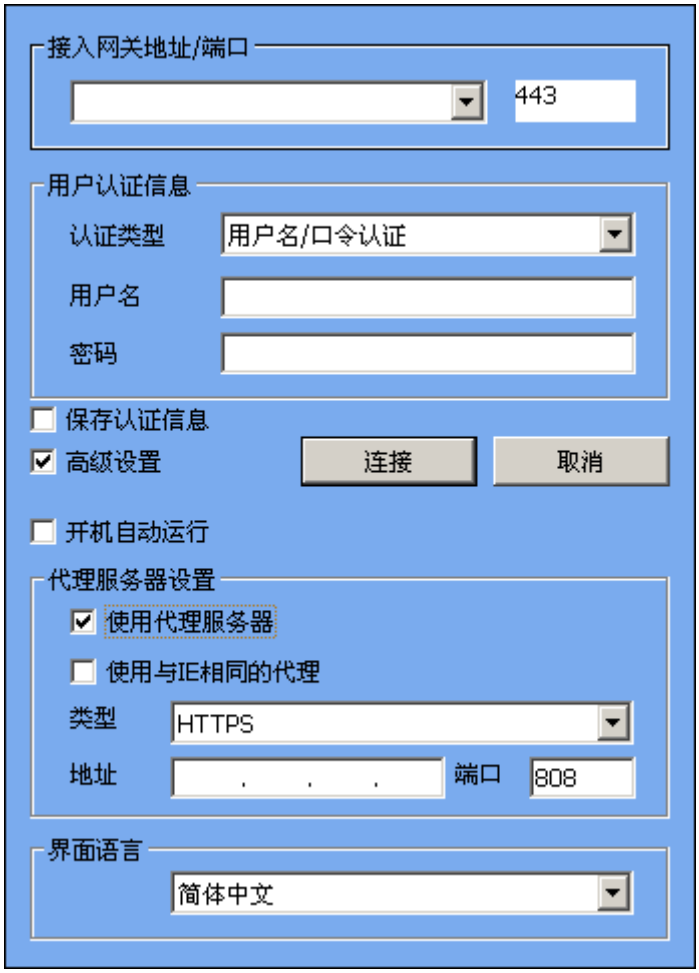
”，弹出天融信 SV 独立客户端的登录窗口，如下图所示。



界面参数说明如下表所示。

参数	说明
接入网关地址/端口	设置 SSL VPN 网关的地址，以及端口转发和全网接入服务运行的端口。 说明： 端口转发服务和全网接入服务均默认运行在网关的 443 端口，一般不需要修改，如需修改，请联系管理员获取该值。
认证类型	选择用户的认证类型：用户名/口令认证、证书认证和双因子认证。
用户名	当用户的认证类型为“用户名/口令认证”或“双因子认证”时，必须输入该用户的用户名。
密码	当用户的认证类型为“用户名/口令认证” 或“双因子认证”时，必须输入该用户的密码。
保存认证信息	选择是否保存用户输入的认证信息，下次登录时无需输入。
高级设置	选择是否配置客户端使用的代理服务器和用户使用的界面语言。 选中“高级配置”后，还需要配置相关参数，请参见后续介绍。

勾选“高级设置”左侧的复选框后，可以配置客户端使用的代理服务器和用户使用的界面语言，界面如下图所示。



界面中有关高级配置参数说明如下表所示。

参数	说明
开机自动运行	选择开机时是否自动运行 SV 独立客户端程序。
使用代理服务器	选择是否通过代理服务器去连接网关，然后访问相应授权资源。天融信 SSL VPN 网关允许用户使用的代理服务器类型主要包括 HTTP 代理、HTTPS 代理和 SOCKS 代理。
使用与 IE 相同的代理	选择是否允许用户使用 IE 浏览器中配置的代理服务器去连接 SSL VPN 网关。 说明： 1）只有勾选了“使用代理服务器”左侧复选框，才能够配置该参数。 2）选中了“使用与 IE 相同的代理”后，用户将使用 IE 浏览器中配置的代理服务器去连接 SSL VPN 网关，SV 独立客户端中配置的代理服务器的“类型”和“地址”无效。
类型	选择用户所使用的代理服务器的类型。 可选值：HTTPS，SOCKS。 说明： 只有勾选了“使用代理服务器”左侧复选框，并且没有选中“使用与 IE

参数	说明
	相同的代理”，才能够配置该参数。
地址	配置代理服务器的 IP 地址。 说明： 只有勾选了“使用代理服务器”左侧复选框，并且没有选中“使用与 IE 相同的代理”，才能够配置该参数。
端口	配置代理服务器的端口号。 说明： 只有勾选了“启用代理”左侧复选框，并且没有选中“使用 IE 代理服务器设置”，才能够配置该参数。
界面语言	选择 SSL VPN 独立客户端界面的语言类型，包括：简体中文、English。可以在中、英文界面之间进行切换。

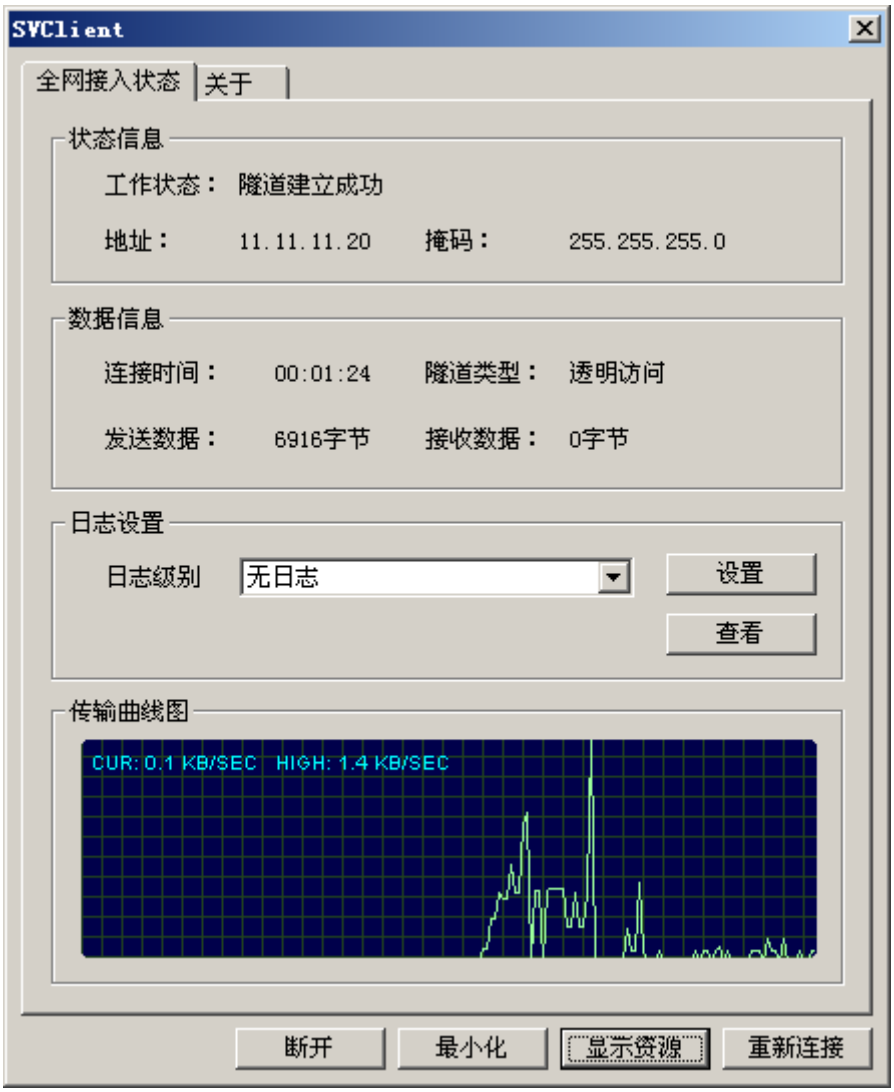
b）设置登录参数，然后点击“连接”按钮，对于使用“用户名/口令认证”方式的用户，可以成功登录到 SSL VPN 网关；对于使用“证书认证”和“双因子认证”方式的用户，还将弹出选择窗口供用户选择已经事先导入到客户主机中的用户证书，然后才能成功登录到 SSL VPN 网关。

用户成功登录 SSL VPN 网关后，SSL VPN 独立客户端以托盘“ ”的形式显示在屏幕右下方。

3．在 SSL VPN 独立客户端使用界面中，查看全网接入客户端的相关参数。

目前，天融信 SSL VPN 网关不支持网关管理员为用户同时开启端口转发模块和全网接入模块，所以只有当管理员为用户开启了全网接入模块，用户登录 SSL VPN 网关后，才能查看全网接入客户端的相关参数，具体操作如下所示：

单击托盘图标或者点击托盘右键菜单项“显示主窗口”后，在弹出的独立客户端的主窗口“SVClient”中激活“全网接入状态”页签，可以查看全网接入客户端的当前状态和连接参数等信息，如下图所示。



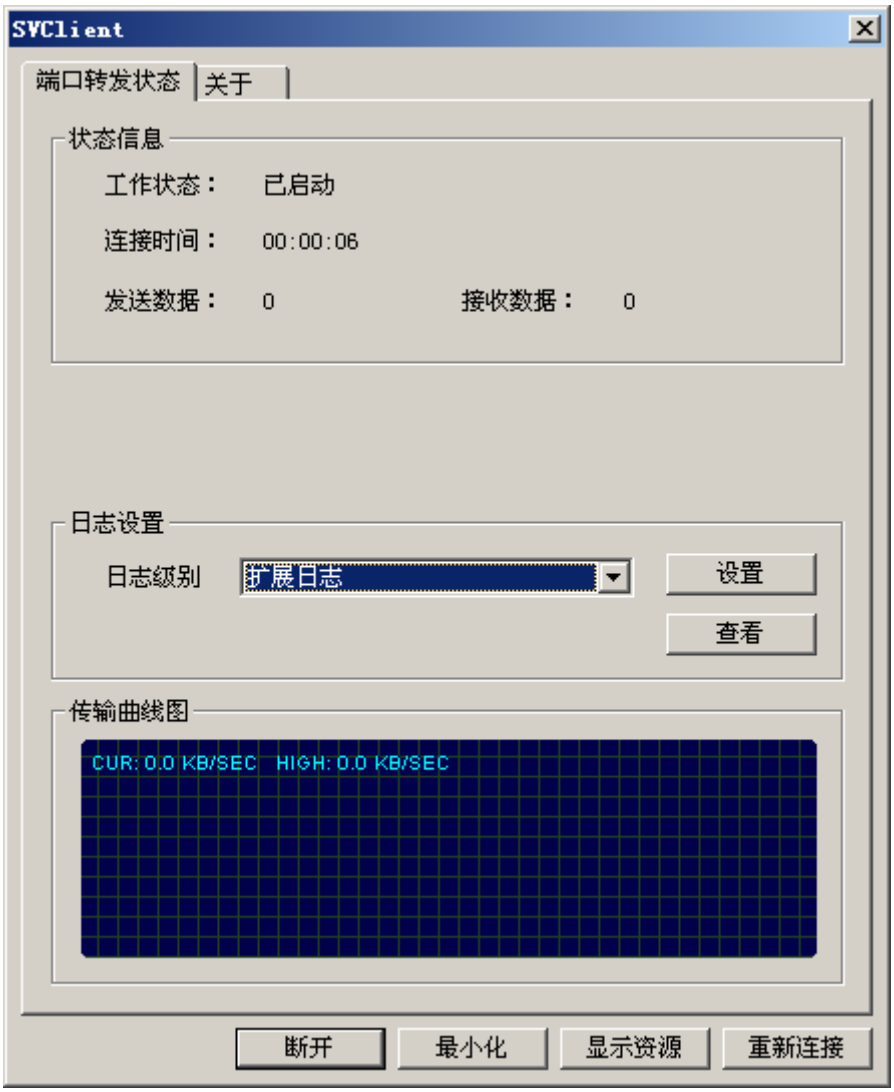
说明

- ✧ “隧道类型”由管理员设定，决定用户可访问资源。若“隧道类型”为“网络隔离”，表明用户端设备完全作为内网设备，远程主机的默认网关设置为虚拟网卡 IP，则原来需要经过默认网关转发的应用都要经过 SSL VPN 网关；若“隧道类型”为“透明访问”，表明用户访问访问内网资源时通过网关转发，不影响用户访问原有的外网资源。
- ✧ “日志设置”一栏中，全网接入日志级别的设置主要用于开发、维护人员定位问题，用户无需关注。

4．在 SSL VPN 独立客户端使用界面中，查看端口转发客户端的相关参数。

目前，天融信 SSL VPN 网关不支持网关管理员为用户同时开启端口转发模块和全网接入模块，所以只有当管理员为用户开启了端口转发模块，用户登录 SSL VPN 网关后，才能查看端口转发客户端的相关参数，具体操作如下所示：

单击托盘图标或者点击托盘右键菜单项“显示主窗口”后，在弹出的独立客户端的主窗口“SVClient”中激活“端口转发状态”页签，可以查看端口转发客户端的当前状态和传输曲线图，如下图所示。



说明

- ✧ “日志设置”一栏中，端口转发日志级别的设置主要用于开发、维护人员定位问题，用户无需关注。

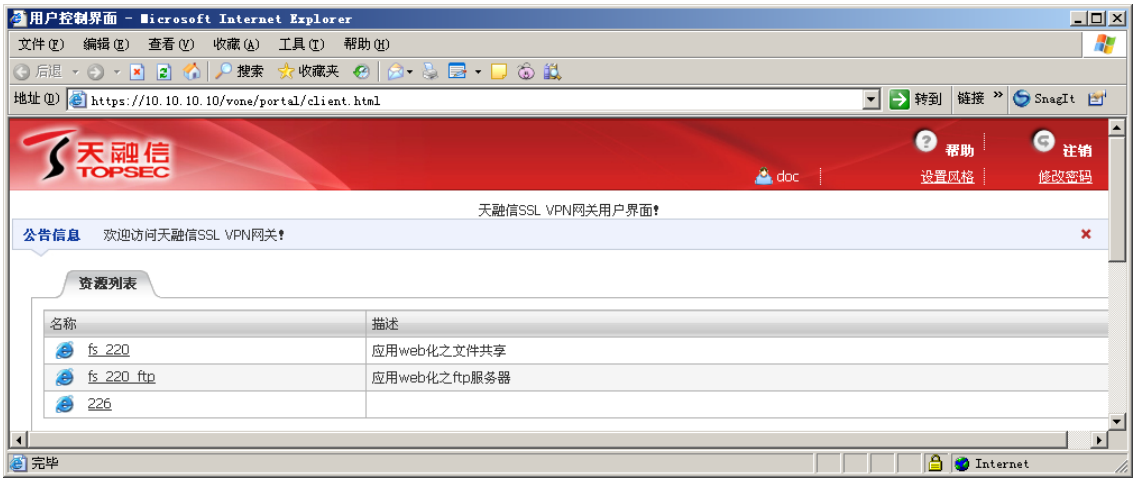
5．在 SSL VPN 独立客户端使用界面中，查看独立客户端软件的相关说明。

在独立客户端的主窗口“SVClient”中激活“关于”页签，可以查看独立客户端的软件名称、版本信息、天融信公司的通信地址以及客服电话等，如下图所示。

6．访问内网资源。

在保证 SV 独立客户端与 SSL VPN 网关正常连接的情况下，用户可以使用网页浏览器或者 C/S 客户端应用程序访问授权资源。

用户可以联系网关管理员获取授权自己访问的内网资源，也可以在独立客户端的主窗口“SVClient”中，点击下方的“显示资源”按钮，进入 web 界面中查看允许显示在用户界面中的授权资源，如下图所示。



对于用户访问内网资源的具体操作，请参见 3.5访问内网资源 的相关介绍，此处不再赘述。

7．重新建立独立客户端与 SSL VPN 网关的连接。

在用户使用过程中，如果发现 SV 独立客户端掉线，则可以点击独立客户端主窗口下方的“重新连接”按钮，以便 SSL VPN 独立客户端与 SSL VPN 网关重新建立连接。

说明

- ✧ 如果管理员开启了自动重连功能，则当全网接入服务异常中断后，可以自动地连续重连。但是当用户点击“断开”按钮，主动停止全网接入功能时，全网接入服务将不会进行重连。

8．断开独立客户端与 SSL VPN 网关的连接。

用户结束授权资源的访问之后，为了安全起见，建议立即断开与 SSLVPN 网关的连接，具体操作如下所示：

a）在独立客户端的主窗口“SVClient”中，点击“断开”按钮，或者直接点击托盘的右键菜单项“断开”，弹出断开天融信 SV 独立客户端的确认窗口，如下图所示。

b）点击确认窗口的“是”按钮即可成功断开连接。

9．将独立客户端的主窗口最小化。

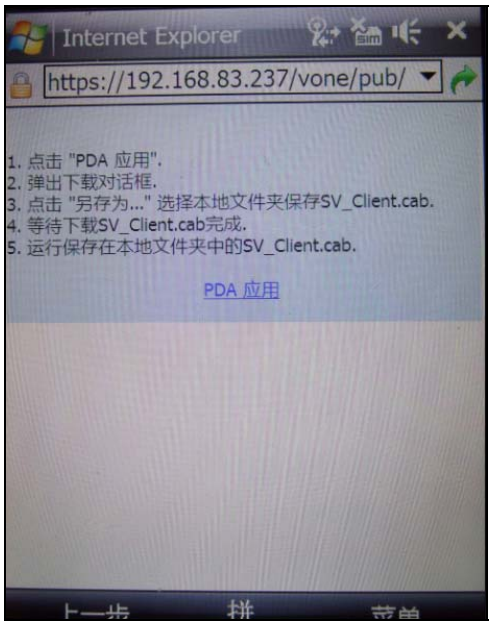
点击主窗口“SVClient”右上方的“×”，或者下方的“最小化”按钮，均可以将 SSL VPN 独立客户端的主窗口最小化到客户主机屏幕的托盘中。

5使用 PDA

天融信 SSL VPN 网关支持远程用户使用 PDA（Personal Digital Assistant，个人数码助理，一般指掌上电脑）登录网关，用户首先需要下载并安装 SSL VPN 客户端程序，然后登录网关访问授权的全网接入资源。下面主要介绍如何使用 PDA 登录网关：

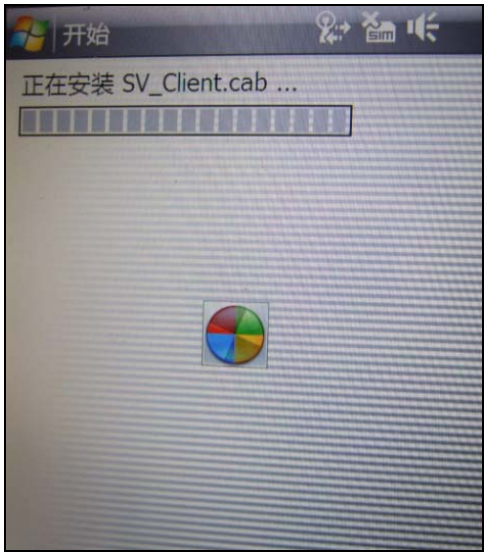
1．安装 SSL VPN 客户端客户端程序。

a）在 PDA 中打开 IE 浏览器，在地址栏内输入“https://SSL VPN 网关的公网 IP”，然后连接到网关，弹出下载 SSL VPN 客户端程序的窗口，如下图所示（图中的网关 IP 仅为示例）。

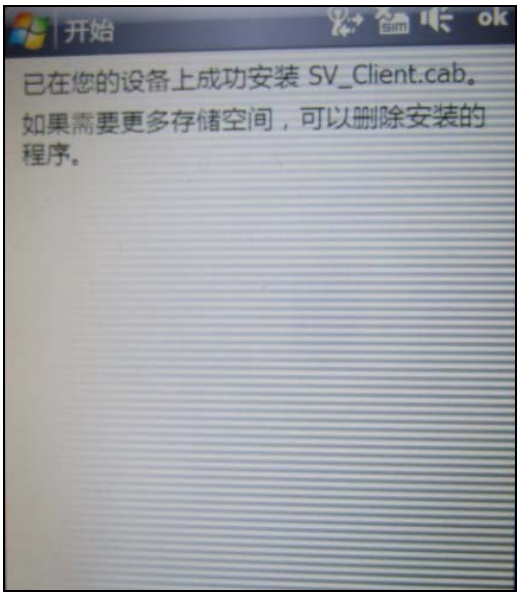


b）点击“PDA 应用”链接，弹出下载 SSL VPN 客户端程序的窗口，如下图所示。

c）选中“下载后打开文件”，然后点击“是”按钮，将 SSL VPN 客户端程序下载到“\My Documents\”目录中，然后自动运行该安装程序，如下图所示。



d）稍后，安装完成，弹出安装成功提示框，如下图所示。

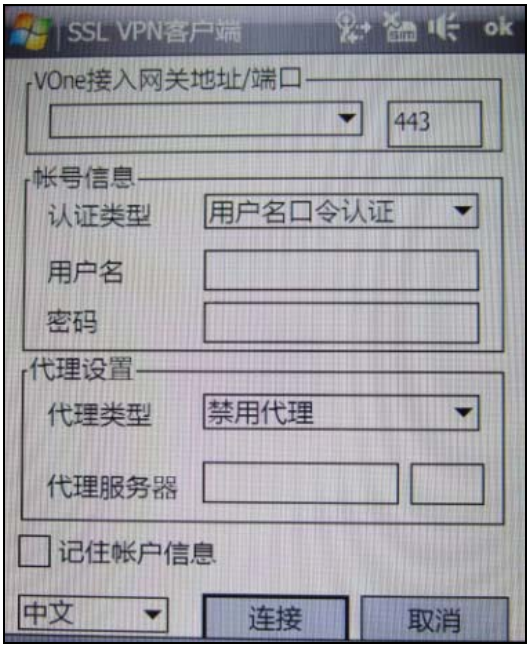


e）关闭该对话框窗口。

2．登录 SSL VPN 网关。

a）在 PDA 中点击 **开始** > **程序**，界面如下图所示。

b）点击“SV_Client”图标，进入 SSL VPN 网关的登录页面，如下图所示。



界面参数说明如下图所示。

参数	说明
VOne 接入网关地址/端口	设置 SSL VPN 网关的地址，以及全网接入服务运行的端口。 说明： 全网接入服务默认运行在网关的 443 端口，一般不需要修改，如需修改，请联系管理员获取该值。
认证类型	选择用户的认证类型：用户名口令认证、证书认证和双因子认证。 说明： 对于证书认证和双因子认证方式，用户必须提前将用户证书导入到 PDA 中。
用户名	当用户的认证类型为“用户名口令认证”或“双因子认证”时，必须输入该用户的用户名。
密码	当用户的认证类型为“用户名口令认证” 或“双因子认证”时，必须输入该用户的密码。
代理类型	用户可以通过代理服务器去连接网关，并通过代理服务器与 SSL VPN 网关建立 TCP/SSL 连接，然后访问相应授权资源。 可选值：禁用代理、HTTPS 代理和 SOCKS 代理。
代理服务器	设置代理服务器的 IP 地址和端口号。
记住帐户信息	选择是否保存用户输入的认证信息，下次登录时无需输入。
中文（或 English）	选择 SSL VPN 客户端界面的语言类型，包括：中文、English。 可以在中、英文界面之间进行切换。

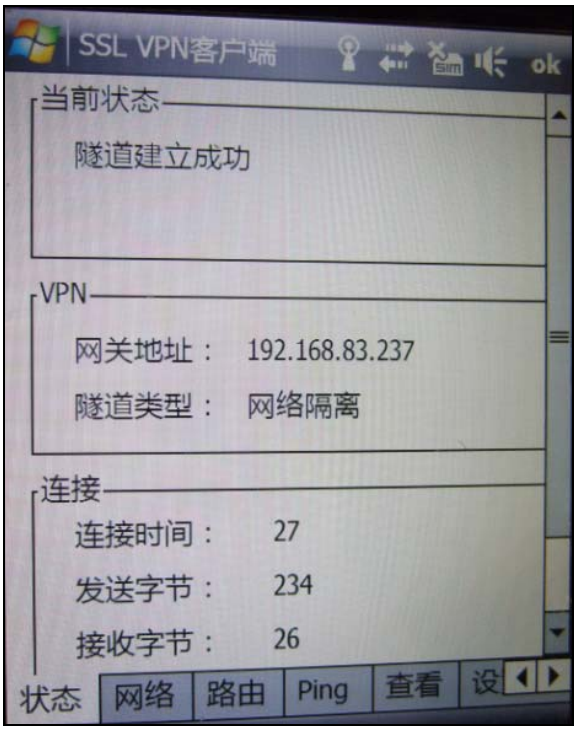
c）参数设置完成后，点击“连接”，对于使用“用户名口令认证”方式的用户，可以成功登录到 SSL VPN 网关；对于使用“证书认证”和“双因子认证”方式的用户，还将弹出选择窗口供用户选择已经事先导入到 PDA 中的用户证书，然后才能够成功登录到 SSL VPN 网关中。

3．在 SSL VPN 客户端使用界面中，访问授权资源。

用户成功登录 SSL VPN 网关后，可以另外打开一个网页浏览器或 C/S 客户端应用程序来访问授权的全网接入资源。

4．在 SSL VPN 客户端使用界面中，查看全网接入客户端的相关参数。

用户成功登录 SSL VPN 网关后，点击“状态”页签，可以查看全网接入客户端的当前状态和连接参数等信息，如下图所示。

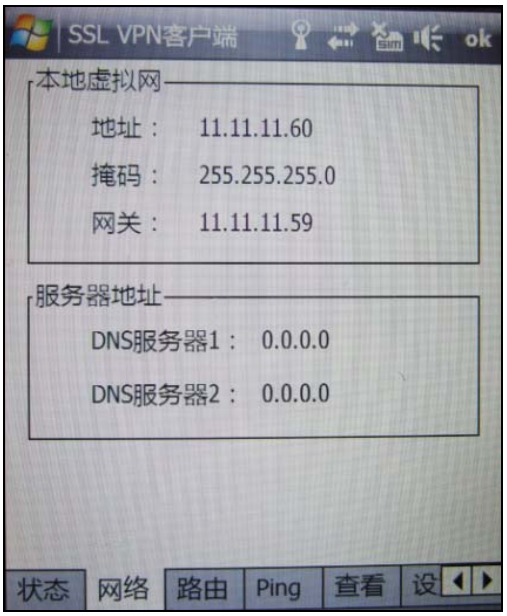


说明

- “隧道类型”由管理员设定，决定用户可访问资源。若“隧道类型”为“网络隔离”，表明用户端设备完全作为内网设备，远程主机的默认网关设置为虚拟网卡 IP，则原来需要经过默认网关转发的应用都要经过 SSL VPN 网关；若“隧道类型”为“透明访问”，表明用户访问访问内网资源时通过网关转发，不影响用户访问原有的外网资源。

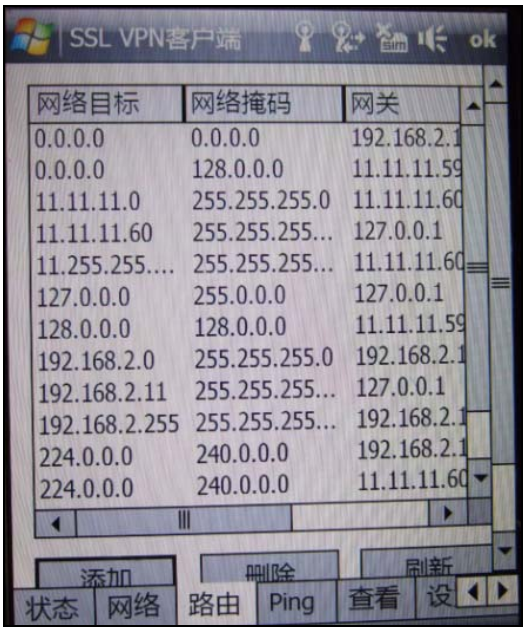
5．在 SSL VPN 客户端使用界面中，查看 PDA 的虚拟网卡以及 DNS 服务器信息。

用户成功登录 SSL VPN 网关后，点击“网络”页签，可以查看 PDA 的虚拟网卡和 DNS 服务器信息，如下图所示。



6．在 SSL VPN 客户端使用界面中，查看 PDA 当前的路由表，同时允许用户添加/删除/刷新路由信息。

a）用户成功登录 SSL VPN 网关后，点击“路由”页签，可以查看 PDA 当前的路由表，如下图所示。



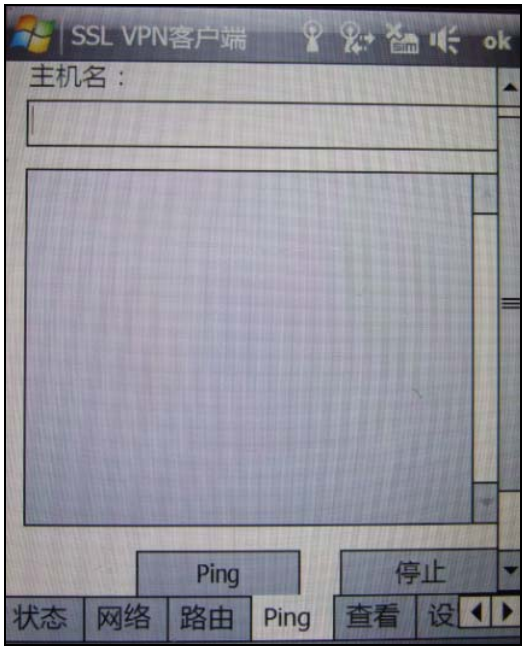
b）点击“添加”，可以添加一条路由信息。

c）选中某条路由，然后点击“删除”，可以删除该路由信息。

d）点击“刷新”，可以刷新路由信息。

7．在 SSL VPN 客户端使用界面中，用户可以进行 Ping 操作，以便探测网络连接状况。

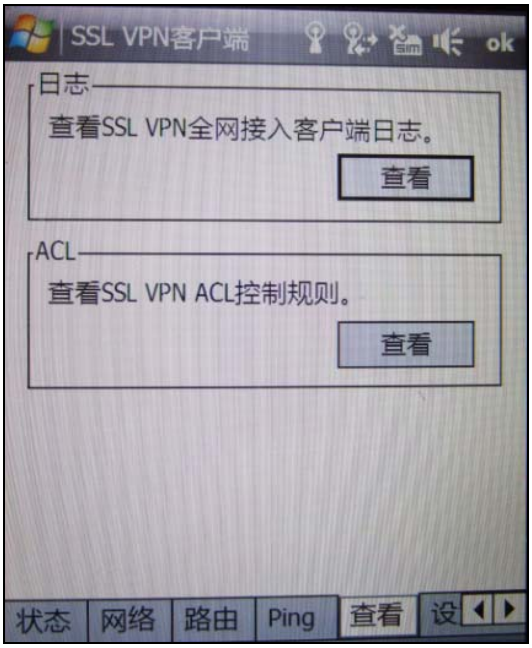
a）用户成功登录 SSL VPN 网关后，点击“Ping”页签，如下图所示。



b）输入主机地址，然后点击“Ping”，可以 Ping 某台主机地址，以便探测网络连接情况。

8．在 SSL VPN 客户端使用界面中，查看 SSL VPN 全网接入客户端日志以及该用户相关的 ACL。

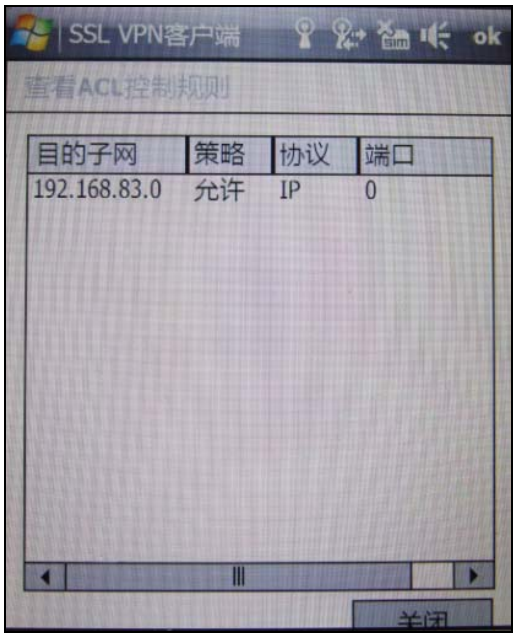
a）用户成功登录 SSL VPN 网关后，点击“查看”页签，如下图所示。



b）点击“日志”一栏的“查看”按钮，可以查看 SSL VPN 全网接入客户端日志，如下图所示。

全网接入客户端日志一般用于开发、维护人员定位问题，用户无需关注。

c）点击“ACL”一栏的“查看”，可以查看该用户相关的 ACL，如下图所示。



9．在 SSL VPN 客户端使用界面中，清除 PDA 中保存的用户登录信息。

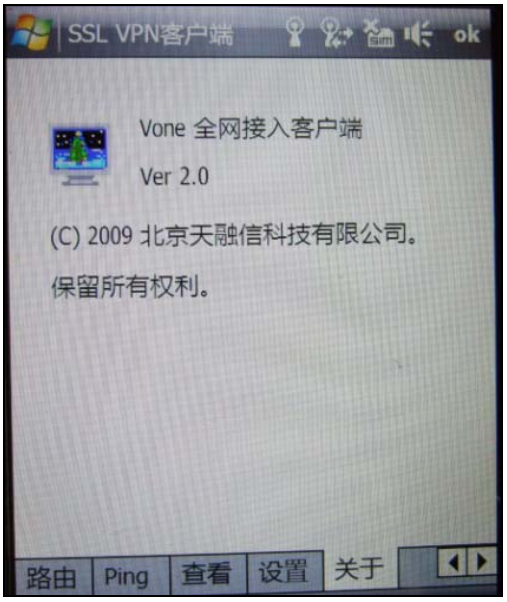
如果在登录页面中选中了“记住帐户信息”，则 PDA 中将保存该用户的登录信息，为了避免用户信息泄露，用户可以手动清除 PDA 中保存的用户登录信息，具体操作如下所示：

a）用户成功登录 SSL VPN 网关后，点击“设置”页签，如下图所示。

b）点击“清除”按钮，可以清除 PDA 中保存的用户登录信息。

10．在 SSL VPN 客户端使用界面中，查看 PDA 中安装的 SSL VPN 客户端程序的相关信息。

用户成功登录 SSL VPN 网关后，点击“关于”页签，可以查看 PDA 中安装的 SSLVPN 客户端程序的相关信息，如下图所示。



声明：

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。

2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。

3. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。

4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。